VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Krištof Danko

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ZÍSKÁVÁNÍ INFORMACÍ O PRŮMYSLOVÝCH ZAŘÍZENÍCH POMOCÍ VYHLEDÁVACÍHO NÁSTROJE
GATHERING INFORMATION ABOUT INDUSTRIAL EQUIPMENT USING A SEARCH ENGINE

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Krištof Danko**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Ondřej Pospíšil**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Krištof Danko ***ID:*** 203450
Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Získávání informací o průmyslových zařízeních pomocí vyhledávacího nástroje

POKYNY PRO VYPRACOVÁNÍ:

Student popíše problematiku bezpečnosti v industriálních sítích, kde se zaměří na bezpečnostní prvky programovatelných logických automatů (PLC) a popíše útoky, které byly v rámci industriálních sítí již realizovány. Student dále popíše možné použitelné komunikační protokoly pro tyto automaty. Následně se zaměří na srovnání vyhledávacích nástrojů pro zařízení připojená do internetu (Shodan, Zoomeye aj.) a okomentuje, jak tyto vyhledávače pracují. V praktické části student srovná jednotlivé vyhledávací nástroje na základě vlastních testů. Dále se student zaměří na získávání informací o průmyslových protokolech pomocí API zvoleného vyhledávače a vytvoří nástroj, kterým bude možné ukládat informace z tohoto vyhledávače do databáze. Student také demonstruje vyhledání vlastního PLC pomocí zvoleného vyhledávače a popíše možné zranitelnosti, které lze využít pomocí zjištěných informací. Nakonec student navrhne možnosti skrytí informací v rámci vyhledávače.

DOPORUČENÁ LITERATURA:

[1] STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. NIST special publication, 2011, 800.82: 16-16

[2] MATHERLY, John. Complete guide to Shodan. Shodan, LLC (2016-02-25), 2015, 1.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: Ing. Ondřej Pospíšil

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Práca sa venuje problematike prevádzkových technológií, so zameraním na bezpečnosť PLC (programovateľný logický automat) a získavanie informácií pomocou vyhľadávacích nástrojov zariadení. Ďalej sú popísané typy a časti priemyselných sietí, ktoré sú hlavným segmentom prevádzkových technológií a vyhľadávače Shodan, Censy, BinaryEdge a Zoomeye. Tieto vyhľadávače sú porovnané na základe dostupných informácií a priemyselných protokolov Siemens S7, Modbus, Ethernet/IP a DNP3. Okrem porovnania vyhľadávačov je v práci vytvorená aplikácie, ktorá dokáže stiahnuť výsledky z vyhľadávača Shodan cez Shodan API a uložiť ich do databázy. Ďalším z bodov práce je zapojenie vlastného PLC za účelom zistenia doby objavenia PLC vo vyhľadávačoch.

KĽÚČOVÉ SLOVÁ

prevádzkové technológie, priemyselné riadiace systémy, PLC, Shodan, Censys, ZoomEye, BinaryEdge, Siemens S7, Modbus, Ethernet/IP, DNP3, API

ABSTRACT

The work is focused on operating technologies, specificaly on the security of PLC (programmable logic controller), and obtaining information using device search engines. The types and parts of industrial networks, which are the main segment of operational technologies, and the search engines such as Shodan, Censy, BinaryEdge, and Zoomeye are described. These search engines are compared based on available information and industry protocols Siemens S7, Modbus, Ethernet / IP, and DNP3. In addition to comparing search engines, this work aims to create an application that can download results from the Shodan search engine via the Shodan API and store them in a database. Another point of work is the connection of own PLC, to determine the time of PLC appearing in search engines.

KEYWORDS

operational technology, industrial control systems, PLC, Shodan, Censys, ZoomEye, BinaryEdge, Siemens S7, Modbus, Ethernet/IP, DNP3, API

DANKO, Krištof. *Získávání informací o průmyslových zařízeních pomocí vyhledávacího nástroje*. Brno, 2021, 89 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: Ing. Ondřej Pospíšil

VYHLÁSENIE

Vyhlasujem, že svoju bakalársku prácu na tému „Získávání informací o průmyslových zařízeních pomocí vyhledávacího nástroje“ som vypracoval samostatne pod vedením vedúceho bakalárskej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád by som poďakoval vedúcemu práce pánovi Ing. Ondřejovi Pospíšilovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Zoznam výpisov

Úvod

Čím ďalej, tým viac priemyselných sieti je pripojených do internetu, aby bolo možné monitorovať, riadiť, a získavať údaje o priemyselných zariadeniach a procesoch z geografických oblastí vzdialených aj niekoľko tisíc kilometrov. Podľa prieskumov IoT Analytics sa predpokladá, že v súčasnej dobe je približne 50 % priemyselných aktív v továrňach pripojených k nejakej forme lokálneho alebo vzdialeného systému zhromažďovania údajov [1].

Bakalárska práca je zameraná na bezpečnosť priemyselných sietí, ich zariadenia pripojených k internetu a na vyhľadávacie nástroje zariadení. Medzi priemyselné zariadenia patria aj programovateľné logické automaty (PLC), na ktoré sa práca zameriava. PLC sa pôvodne používali v interných sietiach, no s pokrokom technológií začiatkom 21. storočia sa začali postupne pripájať aj do verejnej siete napriek tomu, že nedisponujú dostačujúcimi bezpečnostnými prvkami [2]. Vyhľadávacie nástroje zariadení dokážu o týchto zariadeniach vyhľadať citlivé informácie, ktoré dokážu útočníkom výrazne uľahčiť prípravu a útok na PLC. Preto je dôležité vynaložiť maximálne úsilie na zabezpečenie týchto zariadení, poprípade vedieť ako schovať údaje pred vyhľadávačmi zariadení.

Prvým cieľom bakalárskej práce, ktorému sa venuje kapitola 3 a 4 je porovnanie vyhľadávacích nástrojov zariadení pomocou vlastných testov. Následujúci druhý cieľ je vytvorenie aplikácie, ktorá bude pomocou API ukladať výsledky do databázy zo zvoleného vyhľadávača. Výsledok druhého cieľa je popísaný v kapitole 5. Kapitola 6 sa venuje poslednému cieľu práce, ktorým je zapojenie vlastného PLC zariadenia, zistenie, za akú dobu ho dokážu jednotlivé vyhľadávače vyhľadať a navrhnutie skrytia zariadenia pred vyhľadávačmi.

Prvá kapitola sa zameriava na oboznámenie sa z prevádzkovými technológiami, ktoré tvoria jadro v priemyselných sietí. Popisuje priemyselné riadiace systémy, ktoré sú hlavným segmentom prevádzkových technológií, ich ďalšie rozdelenie a komponenty. Následne sú popísané faktory kľúčové pre priemyselné riadiace systémy. Ďalej je popísaná konvergencia prevádzkových a informačných technológii, kde sa nachádza aj príkladná architektúra, ako takýto systém môže vyzerať. V časti bezpečnosť prevádzkových technológii sú spomenuté priemyselné medzinárodné modely, ktoré obsahujú návody a bezpečnostné požiadavky. Následne je spomenutá história útokov na priemyselné siete, hlavne na PLC zariadenia. Posledná časť prvej kapitoly popisuje najbežnejšie sieťové protokoly prevádzkových technológií, ako sú napríklad Siemens S7, Modbus, DNP3. Druhá kapitola je zameraná na vyhľadávacie nástroje zariadení; jedná sa konkrétne o vyhľadávače Shodan, Censys, BinaryEdge a ZoomEye. V kapitole sa nachádza popis základných údajov o tom, ako fungujú a aké funkcie používateľom poskytujú. Nasleduje kapitola, v ktorej sú vyhľadávače

zariadení porovnané. Porovnanie je rozdelené na dve časti, a to porovnanie na základe dokumentácie a informácií z webových stránok vyhľadávačov a porovnanie účtov a výsledkov jednotlivých vyhľadávačov. Popisu práce s API a jeho základnému rozdeleniu sa venuje štvrtá kapitola. V tejto kapitole sa nachádza aj porovnanie a vyhodnotenie práce s API vyhľadávačov, ktoré boli zvolené za najvhodnejšie v predchádzajúcej kapitole. V piatej kapitole je predstavená vlastná aplikácia, ktorá slúži na získavanie výsledkov pomocou REST API z najvhodnejšieho vyhľadávača a ukladá ich do databázy. Posledná, šiesta kapitola popisuje prácu s vlastným PLC zariadením, ktoré bolo zapojené, aby sa zistilo, za ako dlho a aké informácie dokážu vyhľadávače zariadení vyhľadať.

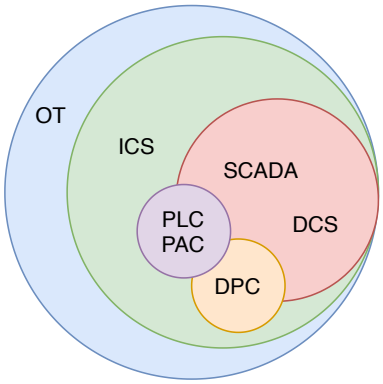
1 Prevádzkové technológie

Keďže je práca zameraná na problematiku kybernetickej bezpečnosti v oblasti priemyselných sietí, je dôležité v práci najskôr definovať a popísať základné vlastnosti týchto sietí, ktoré spadajú do kategórie prevádzkových technológií.

Je dôležité pochopiť rozdiel medzi prevádzkovými technológiami (Operational technology – OT) a informačnými technológiami (Information technology – IT), pretože v súčasnosti v priemyselnom odvetví často dochádza ku konvergencii týchto technológií, a to hlavne vo väčšine stredných a veľkých výrobných podnikoch [3]. IT oddelenia nesú zodpovednosť za všetky počítačové systémy, bez ohľadu na ich použitie. Podpora je centralizovaná, často realizovaná z rôznych lokalít a prostredníctvom organizácií, ktoré majú malé alebo žiadne skúsenosti s automatizáciou a OT sieťami.

IT zahŕňajú celé spektrum dátových modulov, hardvéru a softvéru na vykonávanie rôznych operácií, ako je poskytovanie, ukladanie, obnova, prenos, manipulácia a ochrana údajov a informácii, aby bolo možné dané údaje vymieňať medzi organizáciami.

OT sú systémy riadenia a zabezpečenia zložené z hardvéru a softvéru, ktoré sa používajú na priame monitorovanie alebo riadenie fyzických zariadení, procesov a infraštruktúry. OT boli tiež definované ako technológie, ktoré sú prepojené s fyzickým svetom a zahŕňajú priemyselné riadiace systémy (Industrial control systems – ICS), ktoré zase zahŕňajú systémy riadenia procesov (Process Control System – PCS), distribuované riadiace systémy (Distributed Control Systems – DCS), dozornú kontrolu a získavanie údajov (Supervisory Control and Data Acquisition – SCADA) a mnoho ďalších systémov. Tieto ICS používajú rôzne radiče, ako napríklad programovateľný logický automat (Programmable logic controller – PLC), vzdialené koncové zariadenie (Remote Terminal Unit – RTU), inteligentné elektronické zariadenie (Intelligent



Obr. 1.1: Základné časti prevádzkových technológii [4, 5].

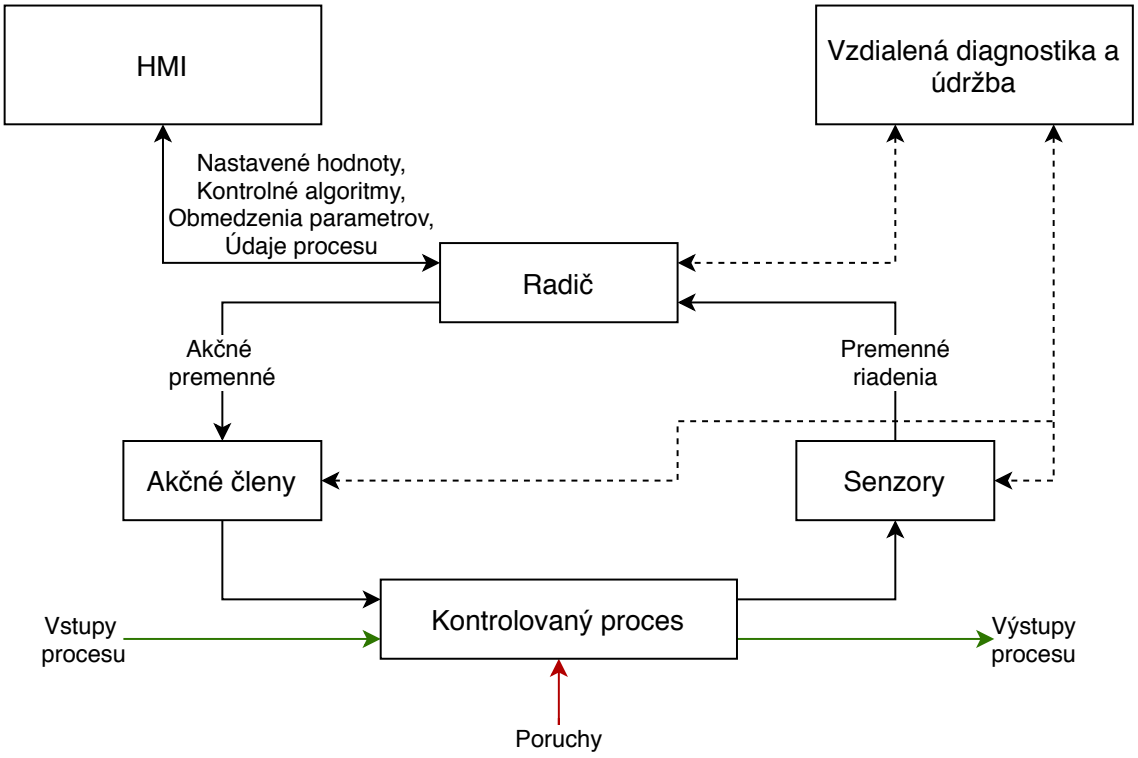
Electronic Device – IED) a ďalšie typy komponentov, ako rozhranie človek–stroj (Human Machine Interface – HMI), komunikačné brány a mnoho ďalších, na vykonávanie určitých procesov. Popísané súčasti OT sú zobrazené na obrázku 1.1.

Hlavnou funkciou OT je zasielanie príkazov do výrobných zariadení a zhromažďovanie spätných väzieb o pokroku priemyselných procesov.

OT siete a systémy sa používajú v rôznych priemyselných odvetviach, ako je energetika, vodné hospodárstvo, produkcia ropy a plynu, doprava, baníctvo a mnoho ďalších. Tieto odvetvia sú súčasťou národných kritických infraštruktúr, bez ktorých by spoločnosť a ekonomika zlyhali, a preto je veľmi dôležitá aj bezpečnosť OT [4, 5, 6].

1.1 Priemyselné riadiace systémy

Priemyselné riadiace systémy (Industrial control systems – ICS) sú významným segmentom v sektore OT; obsahujú rôzne typy zariadení, systémov, ovládacích prvkov a sietí, ktoré úplne alebo čiastočne automatizujú riadiace a monitorovacie procesy vo výrobných a priemyselných zariadeniach. Mnoho dnešných ICS sa vyvinulo vložením IT do existujúcich fyzických systémov, ktoré často nahradili alebo doplnili



Obr. 1.2: Komponenty ICS [7].

mechanizmy fyzickej kontroly. ICS vo všeobecnosti môžu byť veľmi zložité systémy, obsahujúce tisíce rozdielnych komponentov rozmiestnených v rôznych geografických lokalitách a spravujúce zložité procesy v reálnom čase, alebo úplne jednoduché, obsahujúce jedno PLC zariadenie kontrolujúce motor.

Typický ICS obsahuje početné riadiace slučky, HMI a nástroje na vzdialenú diagnostiku a údržbu, vytvorené pomocou sieťových protokolov. Riadiaca slučka využíva senzory, akčné členy a radiče na manipuláciu s riadeným procesom. Senzor je zariadenie, ktoré vykonáva meranie určitých fyzikálnych vlastností a následne tieto informácie posiela do radiča ako premenné riadenia. Radič interpretuje signály a generuje zodpovedajúce akčné premenné na základe nastavených hodnôt, ktoré posiela akčným členom. HMI sa používa na monitorovanie a konfiguráciu nastavených hodnôt, riadiacich algoritmov a na úpravu a stanovenie parametrov v radiči. Taktiež zobrazuje informácie o stave procesu a historické informácie. Vzdialená diagnostika a údržba sa využíva na prevenciu, identifikáciu a zotavenie z abnormálnej prevádzky alebo porúch. Popísané základné fungovanie najbežnejších ICS je znázornené na obrázku 1.2 [7].

1.2 Komponenty priemyselných riadiacich systémov

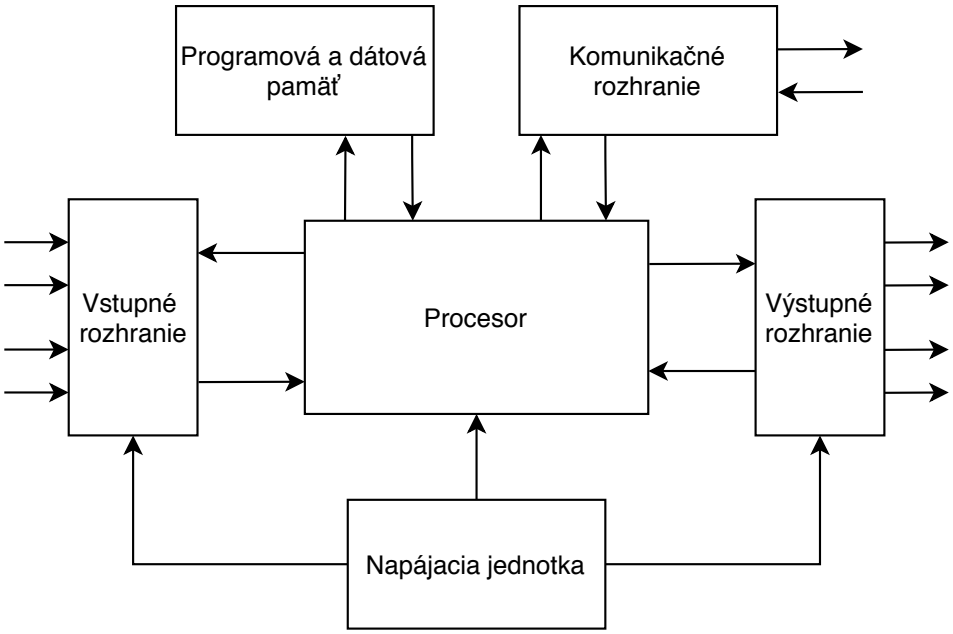
Medzi komponenty ICS patria radiče, softvérové aplikácie, prevádzkové a komunikačné zariadenia. Táto časť popisuje výskyt a všeobecné použitie základných typov radičov a komponentov.

1.2.1 Programovateľný logický automat

Programovateľný logický automat (Programmable logic controller – PLC) je špeciálny typ industriálneho počítača prispôsobeného na riadenie výrobných procesov v reálnom čase, ktoré si vyžadujú vysokú spoľahlivosť, nenáročné programovanie a jednoduchú diagnostiku porúch. Toto zariadenie nepretržite monitoruje vstupné hodnoty z rôznych vstupných snímacích zariadení a produkuje zodpovedný výstup v závislosti od povahy výroby a odvetvia. Typická bloková schéma PLC (obrázok 1.3) sa skladá z piatich častí, a to:

- Centrálna procesorová jednotka (Central processing unit – CPU) – interpretuje vstupné signály, vykonáva riadiaci program uložený v pamäti a vysiela výstupné signály.
- Napájacia jednotka – prevádza striedavé napätie na jednosmerné.
- Pamäťová jednotka – uchováva program, ktorý má vykonať procesor a údaje zo vstupov.

- Vstupné a výstupné rozhranie – príjem a prenos údajov z/do externých zariadení.
- Komunikačné rozhranie – príjem a prenos údajov v komunikačných sieťach z/do vzdialených zariadení.



Obr. 1.3: Bloková schéma PLC[8, 9].

Kompaktné alebo modulárne PLC tvoria základ každého PLC systému. K dispozícii sú v rôznych tvaroch a veľkostiach. Pri malých a jednoduchých systémoch sa používajú malé kompaktné PLC zariadenia, ktoré sú vybavené pevnou konfiguráciou vstupných a výstupných pinov. Ak sa jedná o zložitejšie systémy, vyžaduje to modulárne stojanové PLC zariadenia, ktoré majú možnosť rozšírenia prostredníctvom modulov.

Program PLC pozostáva zo sady pokynov buď v textovej, alebo grafickej podobe, ktorá predstavuje logiku riadiacu proces. Existujú dve hlavné klasifikácie programovacích jazykov, ktoré sa ďalej členia.

1. Textový jazyk
    - Zoznam inštrukcií (Instruction List – IL)
    - Štrukturovaný text (Structured Text – ST)
2. Grafická forma
    - Priečkový diagram (Ladder Diagrams – LD)
    - Funkčný blokový diagram (Function Block Diagram – FBD)
    - Sekvenčný funkčný diagram (Sequential Function Chart – SFC)

Na programovanie PLC je možné použiť všetky tieto programovacie jazyky, avšak grafická forma sa zvyčajne uprednostňuje pred textovou formou.

Od uvedenia prvého PLC zariadenia prešlo mnoho rokov a veľa sa toho zmenilo. Dnes sa s PLC zariadeniami vieme stretnúť od výrobných fabrických strojov cez semafory až po predajné automaty. Najnovšia generácia PLC zariadení má integrovaný Ethernetový port, ktorý sa využíva pri riadení vzdialených vstupných a výstupných modulov, s ktorými komunikuje pomocou protokolov založených na priemyselnom Ethernete, ako sú Modbus/TCP, EtherNet/IP alebo Profinet (viac o komunikačných protokoloch v časti 1.7). Ďalšie využitie je programovanie alebo ladenie programu, poprípade zber údajov z PLC zariadenia [8, 9].

1.2.2 Vzdialené koncové zariadenie

Vzdialené koncové zariadenie (Remote Terminal Unit – RTU) sa vyvíja s podobnými schopnosťami, aké zvyčajne majú PLC zariadenia. RTU sú mikroprocesorom riadené elektronické zariadenia, a na rozdiel od PLC sú určené do vzdialených miest s nepriaznivým prostredím, ako sú vrcholy hôr, ropné plošiny alebo prostredia s vysokou teplotou [10]. Bežné sú dva typy RTU, a to staničné a terénne RTU. Tieto dva typy RTU je možné kombinovať do jedného fyzického RTU.

Terénne RTU prijímajú vstupné signály zo zariadení a senzorov, a s týmito signálmi potom vykonávajú naprogramovanú logiku; zhromažďujú údaje dotazovaním zariadení a senzorov v preddefinovanom intervale. Terénne RTU sú rozhrania medzi zariadeniami alebo snímačmi a stanicou RTU.

Staničné RTU prijímajú údaje od terénnych RTU, a tiež aj príkazy od dozorných radičov. Na základe príkazov a údajov vytvárajú staničné RTU výstupné hodnoty na riadenie fyzických procesov. Riadiace strediská komunikujú výlučne so staničnými RTU [11].

RTU predstavuje hranicu medzi kybernetickým svetom a fyzickými procesmi v reálnom svete. RTU môžu byť programované v jazykoch ako Basic, Visual Basic a C#. Niektoré možno na rozdiel od PLC programovať aj prostredníctvom jednoduchého webového rozhrania; PLC totiž vyžadujú špecifický softvér. RTU je taktiež možné programovať v rovnakých jazykoch ako sú programované PLC. Existuje tiež veľa RTU s predprogramovanými modulmi, ktoré je možné jednoducho použiť pre požadovanú funkciu. RTU môžu komunikovať s riadiacim centrom pomocou WAN technológii, napríklad cez satelit [10].

1.2.3 Inteligentné elektronické zariadenie

Inteligentné elektronické zariadenie (Intelligent Electronic Device – IED) je každé zariadenie, ktoré obsahuje jeden alebo viac procesorov schopných prijímať alebo odosielať informácie z alebo do externého zdroja. Energetické spoločnosti nasadzujú

IED do svojich rozvodní, aby zlepšili automatizáciu a tok informácii do svojich podnikových sietí. Medzi základné funkcie IED patrí ochrana, kontrola, monitorovanie, meranie a komunikácia. IED je možné dopytovať automatizačným procesom v riadiacom centre alebo pomocou terénneho RTU prostredníctvom sériového rozhrania, ethernetu alebo pomocou bezdrôtového spojenia [12].

1.2.4 Inžinierske pracovisko

Inžinierske pracovisko je zvyčajne stolný počítač alebo server so štandardným operačným systémom. Na tomto zariadení sa nachádzajú programovacie softvéry pre radiče a aplikácie. Technici ho používajú na vykonávanie zmien v logike radičov a priemyselných aplikáciach. Automatizačná procesová logika a dáta sú ukladané aj v súbore projektu na tomto zariadení [12].

1.2.5 Rozhranie človek–stroj

Rozhranie človek–stroj (Human Machine Interface – HMI) je softvérová aplikácia, ktorá poskytuje situačné povedomie o automatizačných procesoch operátorovi zariadenia. HMI môže fungovať na rôznych platformách vrátane tabletov alebo telefónov a môže monitorovať viac procesných sieti v jednom momente. Funkcie HMI programujú vývojári na inžinierskych pracoviskách; najbežnejšie bývajú naprogramované tak, aby aj operátor mohol posielať príkazy riadiacemu zariadeniu. HMI typicky zobrazuje model výrobného alebo prevádzkového procesu so stavovými informáciami, ako sú teplota, prietok a hladina vody atď. [12]

1.2.6 Komunikačná brána

Komunikačná brána umožňuje komunikáciu dvoch zariadení s rozdielnou podporou protokolov alebo prenosových médii. Toto zariadenie transformuje dáta z vysielacieho systému tak, aby zodpovedali protokolu a prenosovému médiu cieľového hostiteľa. Jedná sa napríklad o transformácie zo správ Modbus protokolu na sériovej linke na OPC správy v sieti Ethernet [12].

1.2.7 Front–end procesor

Front–end procesor (FEP) je dedikovaný procesor, ktorý sa používa, keď HMI alebo server riadiaceho centra potrebuje získať stavové informácie z viacerých radičov. Vďaka použitiu FEP, doba spracovania a latencie spôsobené spojeniami WAN nebudú rušiť operátora HMI vykonávajúceho riadiace funkcie.

FEP môže obsahovať funkcie komunikačnej brány, ako napríklad prevod z proprietárnych protokolov dodávateľov na otvorené štandardizované protokoly [12].

1.2.8 Historik dát

Historik dát je softvérová aplikácia, ktorá zhromažďuje údaje o procesoch v reálnom čase a ukladá ich do databázy kvôli súbežnej alebo neskoršej analýze. Sú tu uložené rovnaké údaje, aké zobrazuje HMI a každý údaj je označený časovým razítkom. Zvyčajne sa jedná o stolné pracovisko alebo server, na ktorom táto aplikácia beží. Pri niektorých aplikáciach sa môžeme stretnúť s ukladaním údajov do relačných databáz, nejedná sa však o databázový systém, s ktorým sa môžeme stretnúť v IT. Historik dát je navrhnutý pre veľmi rýchle prijímanie údajov bez toho, aby došlo k ich vynechaniu, nepodporuje referenčnú integritu dát a používa protokoly OT. Taktiež môže mať rozhrania, ktoré podporujú komunikáciu pomocou Modbus alebo OPC priamo s HMI, PLC či RTU [12].

1.2.9 Terénne zariadenia

Terénne zariadenia sú senzory, prevodníky, akčné členy a strojové zariadenia, ktoré priamo komunikujú s radičom prostredníctvom digitálneho alebo analógového I/O modulu, ale môžu na komunikáciu s radičom používať aj protokoly OT, ako napríklad Modbus alebo PROFIBUS. Senzory na meranie teploty, vlhkosti, tlaku, zvuku alebo inej fyzikálnej veličiny merajú charakteristiky a reprezentujú tieto informácie v podobe digitálnych alebo analógových signálov. Akčné členy, ako ventilové alebo motorové regulátory, frekvenčné meniče, čerpadlá a mnoho ďalších sa využívajú na vykonávanie fyzikálnych činností [13].

1.3 Typy priemyselných riadiacich systémov

ICS je všeobecný pojem zahŕňajúci niekoľko typov riadiacich systémov, ktoré sú charakterizované podľa ich použitia, ako aj podľa geografického oddelenia medzi radičom a riadiacimi komponentami. Táto časť sa venuje najpoužívanejším typom ICS, ktoré sú popísané z hľadiska ich výskytu a použitia.

1.3.1 Procesný riadiaci systém

Procesný riadiaci systém (Process Control System – PCS), taktiež nazývaný systém založený na PLC riadi automatizačný proces vo výrobnom prostredí, ktorý sa bežne vyskytuje v továrni. PCS je ICS, ktorý monitoruje a riadi procesy na vytváranie samostatných častí alebo na výrobu liekov, palív a chemikálií v nepretržitej výrobe.

Primárnym radičom v konfiguráciách riadiacich systémov je PLC, ktoré poskytuje prevádzkové riadenie diskrétnych procesov. PLC ako riadiaci komponent sa používa aj v SCADA a DCS systémoch. Tieto systémy sa líšia od PCS v tom, že majú aj centrálny riadiaci server a HMI a primárne neposkytujú riadenie v uzavretej slučke bez priameho ľudského zásahu [12].

1.3.2 Bezpečnostný prístrojový systém

Cieľom bezpečnostného prístrojového systému (Safety instrumented system – SIS) je monitorovanie automatizačných procesov a vykonávanie opatrení na zabránenie nebezpečných továrenských stavov alebo operácii. SIS používa snímače, ktoré odosielajú informácie o stavoch do radiča naprogramovaného na uvedenie zariadenia do činnosti tak, aby v prípade poruchy zabránilo nebezpečnému stavu alebo zmiernilo dopady nebezpečných operácii. SIS funguje samostatne a je oddelený od PCS alebo iných systémov z bezpečnostného hľadiska. Ak existuje nebezpečný stav, ktorý ohrozuje personál prevádzky, verejnosť alebo životné prostredie, SIS uvedie systém do bezpečného stavu.

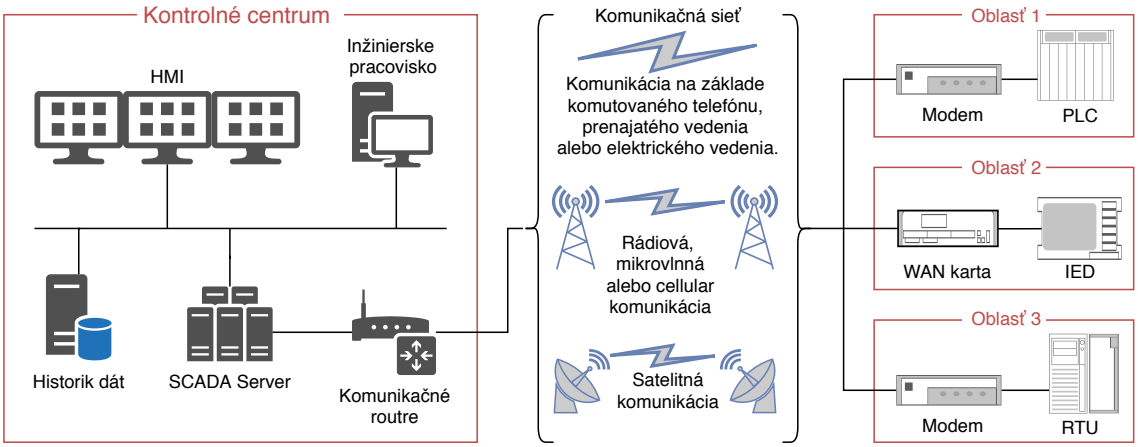
Jednoduchým príkladom, kde by sa SIS mohol vyskytovať je spaľovňa. V prípade zhasnutia plameňa by mohlo dôjsť k nebezpečnému stavu zariadenia, ako napríklad hromadeniu plynu a riziku výbuchu. V takomto prípade by SIS detegoval pokles teploty v spaľovni alebo výskyt plynu v podniku a reagoval by na to odstavením prívodu vykurovacieho plynu [12].

1.3.3 Distribuovaný riadiaci systém

Distribuovaný riadiaci systém (Distributed Control Systems – DCS) sa používa na riadenie viacerých výrobných systémov v rovnakom geografickom umiestnení pre odvetvia ako sú ropné rafinérie, úprava vody a odpadových vôd, elektrárne, chemické výrobné závody a výroba automobilov. DCS môže monitorovať a dohliadať na niekoľko PCS v závode alebo môže riadiť všetku automatizáciu závodu. Vďaka modularizácii produkčného systému, DCS znižuje dopad jednej poruchy na celý systém. V mnohých moderných systémoch je DCS prepojený s podnikovou sieťou, aby poskytoval obchodníkom prehľad o produkcii. Komunikáciu DCS možno charakterizovať ako procesne riadené dotazovanie medzi HMI a PLC. V DCS sa PLC implementujú ako miestne ovládače v rámci dozornej riadiacej schémy [11].

1.3.4 Dozorná kontrola a získavanie údajov

Dozorná kontrola a získavanie údajov (Supervisory Control and Data Acquisition – SCADA) je typ ICS, ktorý zhromažďuje údaje a monitoruje automatizáciu v geografických oblastiach, ktoré môžu byť od seba vzdialené tisíce kilometrov. SCADA systémy sa používajú v distribučných systémoch, ako sú systémy distribúcie vody, ropovody, plynovody, elektrické rozvodné a distribučné systémy, systémy verejnej dopravy a iné. Systémy SCADA integrujú systémy na zber údajov zo systémami na prenos údajov a HMI softvérom a poskytujú centralizovaný monitorovací a riadiaci systém pre množstvo vstupov a výstupov procesu. SCADA systémy sú navrhované tak, aby zhromažďovali informácie z terénu, prenášali ich do centrálneho zariadenia a zobrazovali ich operátorovi graficky alebo textovo, čo mu umožňuje monitorovať alebo riadiť celý systém z centrálneho miesta v takmer reálnom čase. Na základe prepracovanosti a nastavení individuálnych systémov môže byť riadenie jednotlivého systému, operácie alebo úlohy automatické alebo ho môže vykonávať operátor.



Obr. 1.4: Základná topológia SCADA [11].

Základná topológia SCADA, ktorá sa nachádza na obrázku 1.4 zahŕňa riadiaci server, historika dát, HMI a inžinierske pracovisko, ktoré sú umiestnené v riadiacom centre, komunikačné vybavenie a jedno alebo viacero geograficky distribuovaných lokalít pozostávajúcich z RTU alebo PLC, ktoré riadia akčné členy alebo sledujú snímače. Riadici server ukladá a spracováva informácie zo vstupov a výstupov RTU alebo PLC zatiaľ čo riadia lokálny proces. Komunikačný hardvér umožňuje prenos informácii a údajov medzi riadiacim serverom a RTU alebo PLC. Softvér je naprogramovaný tak, aby informoval systém, čo a kedy má monitorovať, aké rozsahy parametrov sú prijateľné a akú reakciu treba iniciovať, keď sa parametre zmenia mimo prijateľných hodnôt.

Okrem RTU alebo PLC sa môžu používať aj IED, ktoré dokážu komunikovať priamo s riadiacim serverom. Kvôli odľahčeniu zaťaženia IED sa používa aj kombinácia terénneho RTU a IED. Terénne RTU dopytuje IED aby zhromaždilo informácie, ktoré následne odovzdá riadiacemu serveru naraz.

Systémy SCADA sú zvyčajne koncipované ako systémy odolné voči poruchám so zabudovanou značnou redundanciou [11].

1.3.5 Systém automatizácie budov

Systém automatizácie budov (Building automation system – BAS) bol kedysi súborom samostatných a nezávislých systémov v budove. BAS v dnešnej dobe monitoruje a riadi služby infraštruktúry budo ako je kúrenie, vetranie, klimatizácia, výťahy, požiarna ochrana a mnoho ďalších [12].

1.3.6 Systém riadenia energie

Systém riadenia energie (Energy management system – EMS) monitoruje a riadi výrobu a prenos elektrickej energie. Je to typ SCADA systému implementovaný na riadenie energetickej siete v rámci štátu alebo medzi národmi.

Najväčší EMS systém je Midcontinent Independent System Operator (MISO), ktorý pokrýva vyše 110 000 km prenosových vedení medzi štátmi USA a jednou kanadskou provinciou [12].

1.4 Návrh priemyselných riadiacich systémov

Návrh ICS, vrátane toho, či sa používajú topológie založené na SCADA, PCS, DCS alebo PLC, závisí od mnohých faktorov. Tieto faktory značne ovplyvňujú dizajn ICS, a tiež pomáhajú určiť bezpečnostné potreby systému. Táto časť sa venuje identifikácii kľúčových faktorov, ktoré ovplyvňujú dizajn pokiaľ sa jedná o vlastnosti riadenia, komunikácie, spoľahlivosti a redundancie ICS. Kľúčové faktory ICS sú [7, 11, 12]:

- **požiadavky riadiaceho načasovania.** Procesy ICS majú širokú škálu časových požiadaviek vrátane veľmi vysokej rýchlosti, konzistencie, pravidelnosti a synchronizácie. Ľudia nemusia byť schopní spoľahlivo a dôsledne splniť tieto požiadavky, a preto sú potrebné automatizované radiče. Niektoré systémy môžu vyžadovať, aby sa výpočet uskutočňoval čo najbližšie k senzorom a akčným členom kvôli zníženiu latencie komunikácie a včasnému vykonaniu potrebných riadiacich činností. Určité ICS sú postavené na operačných systémoch v reálnom čase, kde sú striktné požiadavky na včasnosť. V ICS nie je štandardizovaný reálny čas, ale je zaužívané, že sa jedná o čas do 100 ms.

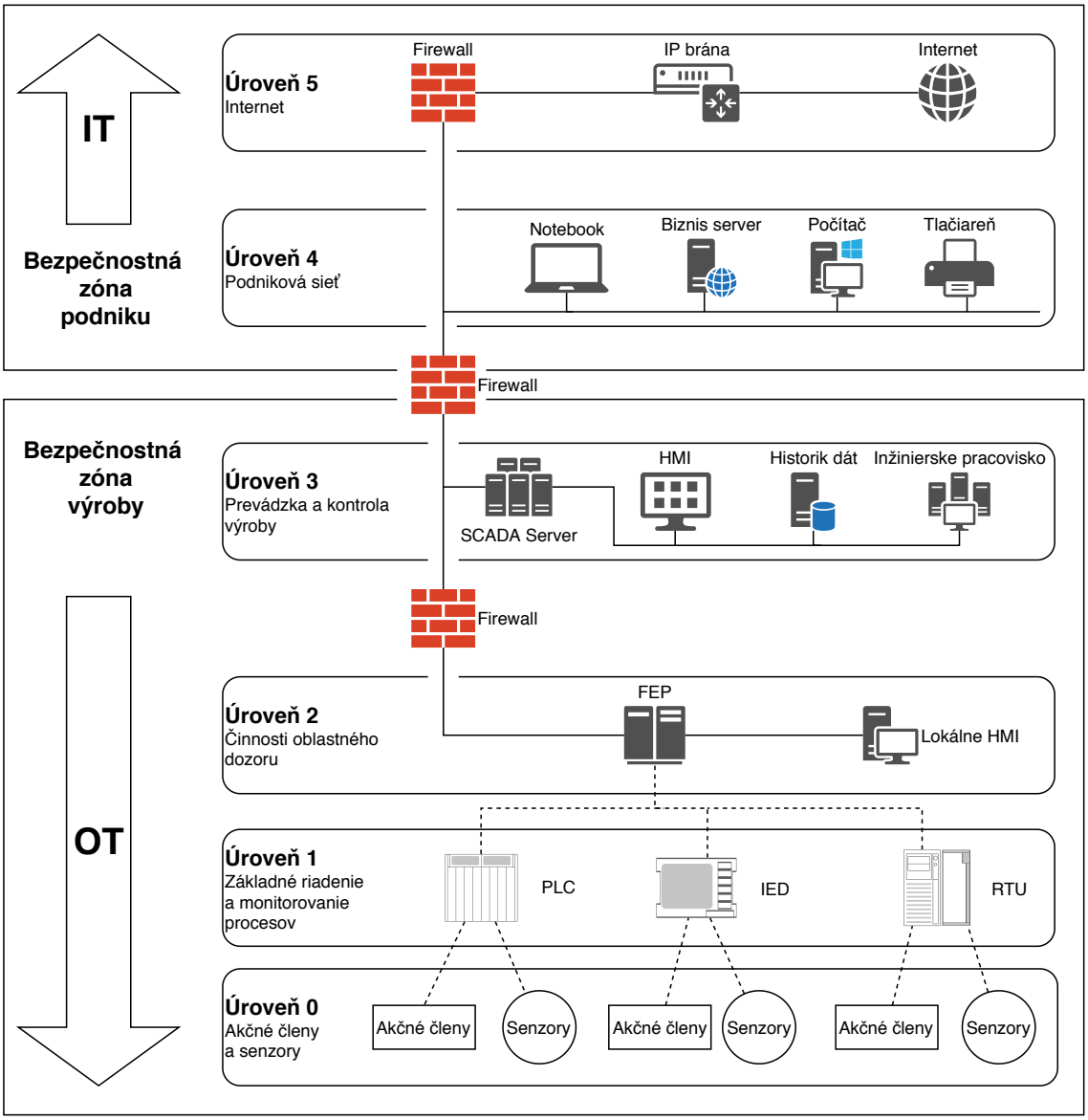
- **Geografická distribúcia.** Systémy majú rôzny stupeň distribúcie od malého systému až po veľké distribuované systémy. Väčšia distribúcia zvyčajne zahŕňa potrebu rozsiahlej oblasti a mobilnej komunikácie.
- **Hierarchia.** Často sa používa hierarchické, inak povedané centralizované riadenie, ktoré poskytuje ľudským operátorom komplexný pohľad na celý systém.
- **Zložitosť riadenia.** Riadiace funkcie je často možné vykonávať pomocou jednoduchých radičov a prednastavených algoritmov. Zložitejšie systémy ako riadenie letovej prevádzky vyžadujú ľudských operátorov, aby zabezpečili, že všetky riadiace činnosti sú vhodné na splnenie cieľov systému.
- **Prístupnosť.** Systémy so značnými požiadavkami na dostupnosť môžu vyžadovať väčšiu redundanciu alebo alternatívne implementácie v celej komunikácii a riadení.
- **Dopad porúch.** Zlyhanie riadiacej funkcie môže mať v rôznych sférach podstatne odlišné dopady. Systémy so závažnejšími dopadmi často vyžadujú schopnosť pokračovať v činnosti prostredníctvom nadbytočných ovládacích prvkov alebo pracovať v zhoršenom stave.

1.5 Konvergencia OT a IT

Existuje mnoho iniciatív, ktoré vedú ku konvergencii IT a OT vrátane technologického pokroku, tlaku na znižovanie prevádzkových nákladov a všadeprítomnej komunikácie. Konvergencia IT a OT znamená, že integrovaný IT a OT systém sa uplatňuje v prácach týkajúcich sa celej siete na výpočet údajov pre zariadenia, proces a plánovanie. Mnoho protokolov OT, napríklad DNP3, pôvodne fungovali cez sériové siete (RS-232), ale konvergenciou sú teraz založené na internetových protokoloch. Moderné protokoly, napríklad IEC 61850, sú však vo veľkej miere založené na nedeterministických, štatisticky multiplexovaných sieťach, ako je napríklad Ethernet. Tieto zmeny umožňujú zariadeniam OT prevádzkovať mnoho sieťových služieb, ktoré sa bežne nachádzajú v IT. Aj keď tieto trendy poskytujú množstvo výhod, pre OT tiež predstavujú určitú mieru rizika.

Na obrázku 1.5 môžeme vidieť tradičnú architektúru ICS s IT a OT konvergenciou. Táto ukážková architektúra obsahuje iba základné časti SCADA systému. SCADA systém je izolovaný od IT a OT siete a následne aj celá topológia od internetu pomocou firewallu. Architektúra systému je rozdelená do niekoľkých samostatných úrovní zabezpečenia.

Úroveň 0 obsahuje fyzické prístrojové vybavenie, ako napríklad ventily, čerpadlá a snímače priemyselných procesov.



Obr. 1.5: ICS architektúra s IT a OT konvergenciou [14, 15].

Na úrovni 1 sa nachádzajú radiče a monitorovacie zariadenia, napríklad PLC, RTU a IED, ktoré sú napojené na fyzické prístrojové vybavenie, ktoré sa nachádza na úrovni 0.

PLC, RTU a IED sú spravované prostredníctvom sieťového pripojenia pomocou FEP ako brány. V tejto topológii slúži FEP na vytvorenie spojenia medzi paketovými IP sieťami a zariadeniami PLC, RTU a IED ktoré sa nachádzajú v sériovej sieti. Moderné PLC majú implementované rozhranie Ethernet; pri takýchto PLC zariadeniach môže byť FEP vynechaný. FEP spolu s HMI sa nachádzajú na úrovni 2 a poskytujú oblastné dohľadné operácie pre sieť riadenia procesov v prostredí miestneho dispečingu.

Funkcie vzdialeného monitorovania a riadenia sa nachádzajú na úrovni 3, ktorá ja pripojená k podnikovej sieti a sieti riadenia procesu cez brány firewall. Na tejto úrovni sa taktiež nachádzajú databázové a historické servery, ktoré sa používajú na zhromažďovanie a ukladanie monitorovaných procesných údajov.

Softvér systému býva naprogramovaný tak, aby automaticky prenášal údaje do podnikových aplikácii, ktoré sú prístupné v podnikovej sieti IT. Podniková sieť sa nachádza na úrovni 4 a je pripojená do verejného internetu, ktorý sa nachádza na úrovni 5, cez bránu firewall.

Pripojenie predtým oddelenej siete OT k internetu prostredníctvom siete IT okamžite vystavuje sieť OT a všetky pripojené zariadenia OT k rôznym hrozbám, ktoré v IT priestore existujú roky. OT vo všeobecnosti nie sú bezpečné, pretože boli navrhované s predpokladom, že nebudú vystavené hrozbám z IT siete. Nárast vzdialeného prístupu tretích strán k sieťam OT navyše ďalej rozširujú povrch útokov a vytvárajú nové chyby zabezpečenia [14].

1.6 Bezpečnosť OT

Priemyselná automatizácia už nie je obmedzená stenami výrobnej fabriky. Stále viac automatizácii sa projektuje tak, aby bola možná komunikácia zo vzdialených bodov, ktoré sú vzdialené niekoľko desiatok až stoviek kilometrov. Takáto komunikácia umožňuje hackerom využívajúcim rôzne zraniteľnosti útočiť na prevádzkové technológie za cieľom získavania údajov a spôsobovania škody vo výrobe.

Bezpečnosť systémov OT má dva zdroje bezpečnostnej špecifikácie; jeden pre nasadenie OT systémov na všeobecné účely a druhý súbor požiadaviek, ktoré sú požadované osobitne segmentáciou infraštruktúry.

Pre systémy na všeobecné účely existujú priemyselné medzinárodné modely, ako napríklad IEC 62443 pôvodne označovaný ANSI/ISA-99 [16, 17]. NIST vydal dokumenty NIST 800-82r2 [11], NIST 800-53r5 [18] a tiež systémový ochranný profil (SPP) [19] pre priemyselné riadiace systémy, ktoré obsahujú návody na funkčné a bezpečnostné požiadavky týchto systémov.

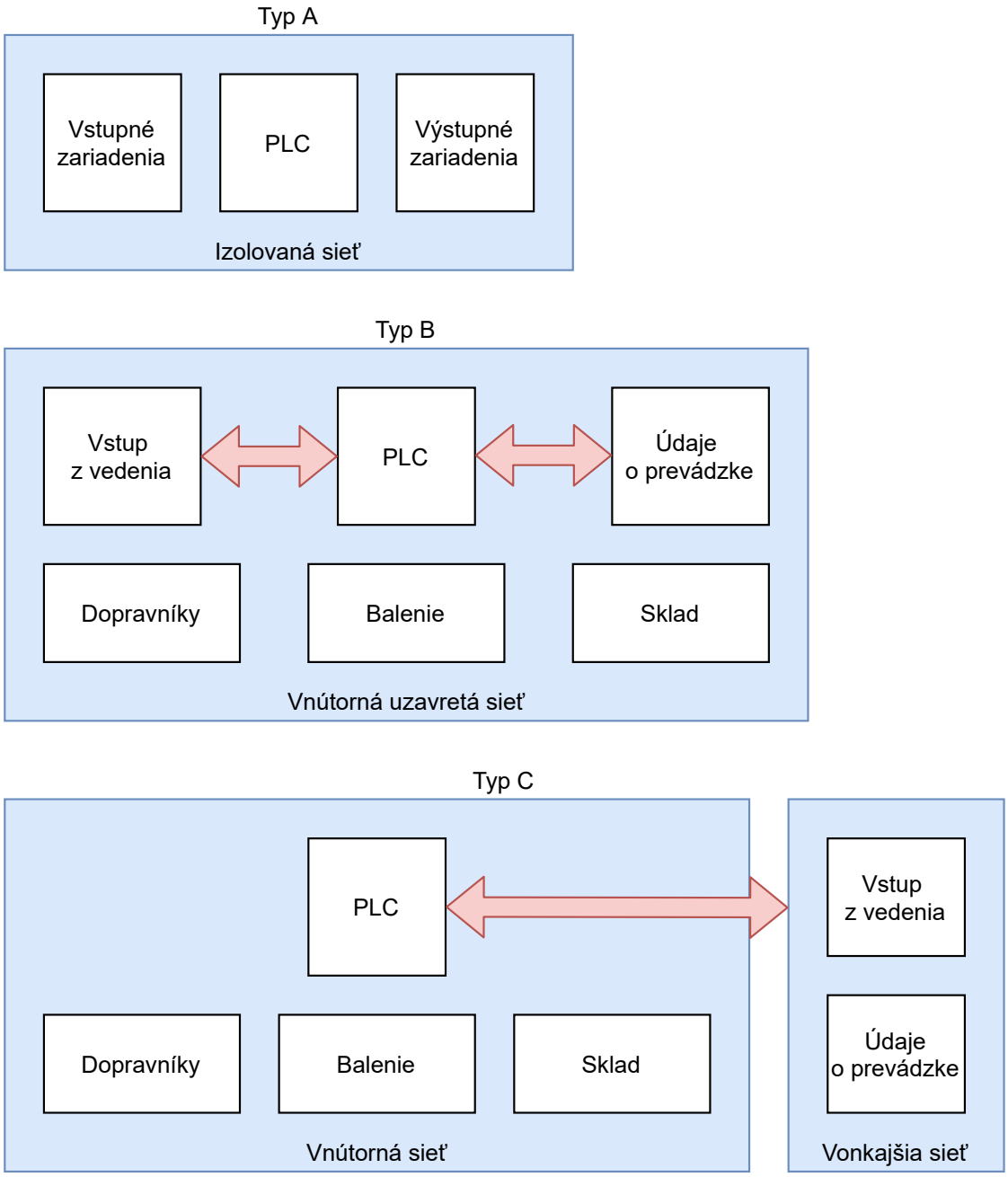
V prípade segmentácie infraštruktúry v oblasti bezpečnosti v prostredí riadiacich systémov existuje množstvo rôznych štandardov, ako napríklad API Std 1164 [20] pre ropné a plynné SCADA systémy, NRC Regulatory Guide 5.71 [21] pre jadrové zariadenia, CFATS and RBPS [22] pre chemické zariadenia a mnoho ďalších, ktoré môžu ale nemusia platiť na základe odvetvia a ďalších faktorov. Tieto štandardy sa veľmi líšia a tie, ktoré sa používajú sa nevyberajú na základe operátora, ale skôr reguláciou založenou na zosúladení odvetvia.

Bezpečnosť OT systémov záleží aj od bezpečnosti jednotlivých komponentov, ktoré sa v danom systéme nachádzajú. Mnoho zariadení, ako napríklad staršie PLC,

RTU alebo IED nemusia obsahovať možnosti zabezpečenia a v novších zariadeniach sa môžu vyskytovať chyby, ktoré môžu rôzne exploity zneužiť. Najčastejšie sú exploity zamerané na PLC zariadenia od firmy Siemens, čo môže byť z toho dôvodu, že okolo 80 % PLC zariadení na trhu je predaných od siedmych spoločností na svete. Najväčší podiel na trhu má spoločnosť Siemens s 30,7 % podielom, nasleduje druhá spoločnosť Rockwell Automation s 21,6 % a na tretom mieste je spoločnosť Mitsubishi s 13,9 %. Štvrté až siedme miesto patrí spoločnostiam Schneider Electric s 8,9 %, Omron s 6,6 %, GE Fanuc s 4 % a Moeller s 2,3 % podielom [23]. Voľne prístupné exploity sú staré a chyby, ktoré využívali, vývojári softvéru už opravili. Tieto exploity sa ale dajú použiť na zariadenia so starším operačným systémom. Existujú však aj firmy, ktoré vyvíjajú exploity a následne ich predávajú a pravidelne ich aktualizujú. Ruská firma GLEG ponúka SCADA+ balíček, ktorý obsahuje okolo 350 exploitov pre SCADA systémy a ich komponenty, ktorý bol naposledy aktualizovaný 11.05.2021 [24]. V tomto balíčku sa nachádzajú aj exploity pre zraniteľnosti nultého dňa. Zraniteľnosti nultého dňa sú zraniteľnosti v zabezpečení softvéru, ktoré boli nahlásené, ale vývojári ich ešte neopravili.

Z hľadiska bezpečnosti PLC zariadení môžeme kategorizovať tri rôzne typy sietí, kde sa PLC používajú. Typ A je izolovaná sieť pre daný stroj, kde je PLC oddelené od akejkoľvek siete. K PLC je pripojený iba stroj a HMI, vďaka ktorému je možné vykonávať obsluhu samostatného stroja. Sieť typu B je interná sieť fabriky, ktorá je obmedzená na uzavretú oblasť a typ C je sieť, do ktorej je možné pristupovať aj z verejnej siete. Rozdelenie sieti so základnými prvkami siete je možné vidieť na obrázku 1.6.

PLC hrozby možno rozdeliť na základné, pokročilé a pokročilé trvalé hrozby (Advanced Persistent Threat – APT). Základné hrozby môžu byť všeobecné phishingové podvody alebo útoky proti organizáciám s nízkou alebo žiadnou bezpečnosťou. Techniky útoku sú k dispozícii na internete alebo sa jedná o open-source softvér. Pokročilými hrozbami môžu byť DDoS (Distributed denial of service – Distribuované odmietnutie služby), získavanie súkromných dát alebo vydieranie pomocou vlastných nástrojov a techník za účelom zisku. APT hrozby sú vytvárané sofistikovanými protivníkmi, ktorí obchádzajú súčasné osvedčené postupy pomocou viacerých nástrojov. Typmi hrozieb môžu byť útočníci, operátori botnetov, zločinecké skupiny, zahraničné spravodajské služby, insideri (zamestnanci, dodávatelia, obchodní partneri), phisheri, spameri, autori škodlivého softvéru, teroristi a priemyselní špióni [25].



Obr. 1.6: Typy sieti z hľadiska bezpečnosti PLC [25].

Samostatné útoky na PLC zariadenia sa delia podľa toho, čo jednotlivé typy hrozieb napadajú, a to na [26]:

- **útok na úpravu firmvéru** – útočník nahrá nový firmvér do PLC
- **útok na manipuláciu s konfiguráciou** – útočník upraví logiku
- **útok na riadenie toku** – útočník nájde v PLC pretečenie vyrovnávacej pamäte alebo RCE
- **útok obídenia autentifikácie** – útočník nájde spôsob obísť autentifikáciu.

Prí útokoch na PLC zariadenie, môžu byť útoky rozdelené aj z hľadiska prístupu útočníka k PLC. Prvou kategóriou sú útoky, keď má útočník priamy prístup k PLC zariadeniu. Ak sa jedná o útoky, keď útočník nemá priamy prístup k PLC zariadeniu, môžeme rozdeliť útoky na dve kategórie. Prvá kategória pri nepriamom prístupe k PLC je útok z vnútornej priemyselnej siete, keď je útok vykonávaný cez prvok siete ako HMI, komunikačný server, inžinierske pracovisko atď. Druhou kategóriou je útok z verejnej siete, keď sa používajú viaceré sofistikované nástroje a technológie. V nasledujúcich podkapitolách sú podrobnejšie rozobraté jednotlivé kategórie; nachádza sa v nich popis o akých útočníkov sa jedná, aké postupy využívajú a na aké PLC siete z hľadiska bezpečnosti sa útočí.

Priamy prístup k PLC zariadeniu

Útoky, kedy má útočník priamy prístup k PLC zariadeniu sú najčastejšie pri sieťach typu A. Pri sietiach typu B a C sa z bezpečnostných dôvodov PLC umiestňujú do miestností, kde môžu vstupovať iba vybraní zamestnanci. PLC zariadenia v sieti typu A sú vystavované najväčšiemu riziku zo strany zločineckých skupín, priemyselných špiónov a insiderov. Z ohľadom na tento typ útočníkov môžeme PLC označiť ako zariadenia s vysokým rizikom zraniteľnosti.

Zločinecké skupiny pôsobia s cieľom peňažného zisku. Pri priamom prístupe k PLC môže prísť k odcudzeniu alebo znehodnoteniu, čo má za následok odstavenie stroja a firmy prichádzajú o finančné zisky.

Priemyselní špióni patria do rovnakej kategórie až na to, že po útoku ostáva PLC nepoškodené a plne funkčné. Ich cieľom je duševné vlastníctvo a know–how.

Insideri vzhľadom na menšie prekážky v prístupe k zariadeniu môžu predstavovať hrozbu. Výhodou insiderov je dôkladné poznanie cieľa; aj pri základných zručnostiach dokážu znehodnotiť PLC alebo vymeniť pamäťovú kartu za účelom finančného zisku, poprípade osobného uspokojenia.

Útočníci pri priamom prístupe k PLC patria do kategórie základných a pokročilých hrozieb a sú označovaní ako vysoko rizikoví [25, 27].

Nepriamy prístup k PLC zariadeniu – útok z vnútornej siete

Útoky z vnútornej siete sú rovnako nebezpečné pre siete typu B a C, ktoré čelia rovnakým hrozbám ako pri útokoch s priamym prístupom k PLC. Útočníci s priamym prístupom k PLC sú v týchto sieťach označovaní taktiež za vysoko rizikových a to aj v prípade, že môžu čeliť väčším prekážkam pri prístupe k PLC. Insideri v sieťach typu B a C kradnú heslá iných technikov, pomocou ktorých sa prihlasujú do inžinierskeho pracoviska, cez ktoré sa dajú konfigurovať PLC zariadenia. Pomocou

pracoviska vydávajú pokyny na vypnutie PLC, čím spustia čiastočné vypnutie výrobného procesu. Okrem týchto útočníkov sú pri útokoch z vnútornej siete rizikoví aj phisheri, autori škodlivého softvéru, teroristi a zahraničné spravodajské služby. Títo útočníci sú klasifikovaní so stredným rizikom pre hrozby, ktoré pri sietiach typu A majú nízke riziko, pretože rozsah vzdialeného prístupu je stále obmedzený na kontrolovanú oblasť bez priameho prístupu na internet.

Phisheri využívajú podvodnú techniku na internete, takzvaný phishing k získaniu citlivých údajov ako sú prístupové heslá, informácie o objekte alebo možný prístup k zariadeniam pomocou elektronickej komunikácie. Pre získanie dôvery útočníci predstierajú, že sú IT, OT administrátori alebo nadriadení pracovníci. V takejto komunikácii sa často vyskytujú gramatické chyby alebo sú zasielané z mierne pozmenených e-mailových adries, ktoré si pracovníci nemusia všimnúť. Tieto hrozby sú klasifikované ako základné a pokročilé.

Autori škodlivého softvéru sú útočníci, ktorí najčastejšie vytvárajú jednoduché DoS vírusy alebo programy, ako napríklad mazanie pevných diskov alebo záplava SYN paketov. Tieto programy sú do vnútornej siete prenášané pomocou USB kľúčov, prípadne útočníci využívajú Cell–phone WIFI útok. Tento spôsob nabúrania sa do systému patrí medzi pokročilé a APT hrozby. Cell–phone WIFI je útok, kedy je vytvorená užitočná, atraktívna a bezplatná aplikácia pre mobilné zariadenia. Aplikácia je následne cielená na pracovníkov kritických infraštruktúr, aby si stiahli bezplatnú aplikáciu, ktorá beží nepretržite na pozadí a skenuje dostupné WI-FI siete. Niektoré z týchto sieti chránených heslom sú súčasťou priemyselných riadiacich systémov. Útočníci následne pomocou phishingových útokov získavajú heslá a cez napadnuté mobilné zariadenia kompromitujú činnosť tovární, čo vedie k neplánovanému odstaveniu. Mobilné zariadenie sa následne odpojí od siete WI-FI a tento útok sa pravidelne opakuje [28].

Teroristi sú skupina útočníkov, ktorých hlavným cieľom pri ICS sieťach sú veľké finančné straty alebo straty na ľudských životoch. Jedným z možných útokov týchto skupín s cieľom poškodzovania ICS siete je Sophisticated Credentialed ICS Insider. Skupina útočníkov podpláca alebo vydiera ICS insidera, ktorý systematicky odovzdáva informácie o návrhu fyzických procesov, riadiacich systémov a bezpečnostných konfigurácií. Útočníci vyvíjajú vlastný autonómny malvér navrhnutý tak, aby dokázal obísť nasadené konfigurácie zabezpečenia. Insider zámerne uvoľní malvér v systéme, ktorý sa neskôr aktivuje. Pomocou nasadeného malvéru môže dôjsť k explózii, ktorá zabije niekoľko pracovníkov, spôsobí miliardové škody a odstaví podnik na niekoľko mesiacov. Jedná sa o útočníka s vysokou mierou sofistikovanosti, ktorý má vysoký stupeň technickej vyspelosti, vie zistiť aké kybernetické útoky systémy bezpečnosti a ochrany zariadenia očakávajú najmenej a ako tieto ochrany prekonať [28]. Z tohoto dôvodu sú tieto hrozby v kategórii pokročilých a APT hrozieb.

Zahraničné spravodajské služby majú zdroje a podporu zo strany štátu na zabezpečenie značného fyzického, sociálneho a ekonomického dopadu na ostatných. Tieto služby sú preto schopné využívať všetky doposiaľ spomenuté útoky, ktoré patria do pokročilých ale hlavne APT hrozieb. Zahraničné spravodajské služby a teroristi sa zameriavajú na kritickú infraštruktúru, a preto ich siete typu A moc nezaujímajú [25, 27].

Nepriamy prístup k PLC zariadeniu – útok z verejnej siete

Medzi najčastejšie útoky na ICS siete a samostatné PLC zariadenia patria útoky z verejnej siete. Všetky útoky z verejnej siete sú cielené na siete typu C, kde je široká konektivita a ako jediná sieť z hľadiska bezpečnosti PLC je pripojená do internetu. Pre siete typu C sú všetky doposiaľ spomenuté typy hrozieb klasifikované ako vysoko rizikové. Okrem vyššie spomenutých typov hrozieb sú pri útokoch z verejnej siete nebezpeční aj útočníci, spameri a operátori botnetov, ktorí sú taktiež klasifikovaní ako vysoko rizikoví.

Útočníci sa zaraďujú pod typ hrozby, ktorá kompromituje systémy pre spokojnosť jednotlivcov. Útočníci môžu byť používatelia jednoduchých skriptov voľne dostupných na internete a nemusia mať schopnosti zamerať sa na bezpečnejšiu kritickú infraštruktúru. Tieto útoky sú klasifikované ako základné hrozby.

Nevyžiadané masovo šírené e-maily, komentáre alebo súkromné správy, takzvaný spam, využívajú spameri na prienik malvérov do systémov. Spam patrí do kategórie základných alebo pokročilých hrozieb. Tieto spamy obsahujú URL odkazy, keď po kliknutí na daný odkaz sa malvér stiahne do zariadenia a následne napadá jednotlivé ICS komponenty vo vnútornej sieti.

Botnet je sieť počítačov infikovaných špeciálnym softvérom, ktorý je riadený z jedného centra. Botnety využívajú útočníci, ktorí sa nazývajú operátory botnetov. Operátory botnetov najskôr napadajú počítače, ktoré sa môžu nachádzať aj vo vnútornej ICS sieti, a keď je počet infikovaných PC staníc dostatočný, začnú útočiť na PLC zariadenia alebo iné ICS prvky, napríklad DDoS útokom. Operátory botnetov sú o niečo sofistikovanejší ako útočníci a pri svojich útokoch používajú rôzne systémy a siete, preto sú zaradení do kategórie pokročilých hrozieb [25, 27].

1.6.1 História PLC útokov

Prvé verejne dostupné informácie o zraniteľnostiach v komponentoch ICS pochádzajú z roku 1997, kedy boli zverejnené prvé dve zraniteľnosti. Odvtedy sa počet každoročne odhalených zraniteľnosti výrazne zvýšil. Prvý známy útok na PLC, Stuxnet, bol objavený v roku 2010 a zapríčinil obdobie prudkého rastu zraniteľností

v rokoch 2010 až 2012. V tabuľke 1.1 sa nachádzajú známe útoky na PLC zariadenia, ktoré mali voľno dostupné dokumentácie. Posledné útoky s voľno dostupnými dokumentáciami sú z roku 2016 a novšie sa nepodarilo nájsť. Útoky z tabuľky sú podrobnejšie rozobraté v podkapitolách.

Meno	Rok	Predpokladaný cieľ
Stuxnet	2010	Iránske zariadenia na obohacovanie jadrového paliva
Duqu / Duqu 2.0	2011/2015	Dokumenty priemyselných projektov
BlackEnergy	2015	Ukrajinská elektráreň
Ghost in PLC	2016	–
Industroyer (CrashOverride)	2016	Ukrajinská elektráreň
Kemuri	2016	Vodárenská spoločnosť
PLC-Blaster	2016	–
LogicLocker	–	–

Tab. 1.1: Výpis významných útokov na PLC.

Výskumné práce

Útoky, pri ktorých nie sú napísané predpokladané ciele sú výskumné práce, ktoré majú poukázať na nedostatky PLC zabezpečenia. V tabuľke 1.1 sa nachádzajú tri takéto útoky, ktoré boli prezentované vo výskumných prácach, a to Ghost in PLC, PLC-Blaster a LogicLocker.

Ghost in PLC je nezistiteľný rootkit PLC zariadenia pomocou Pin Controll útoku. Útok v zásade spočíva v zneužití funkcií kontroly pinov zabudovaného systému za behu. Útočník môže buď blokovať komunikáciu s perifériami, spôsobiť im fyzické poškodenie alebo manipulovať s načítanými alebo zapísanými hodnotami z periférií – viac v literatúre [29].

PLC-Blaster je červ, ktorý je umiestnený a beží iba na PLC a k rozmnožovaniu nevyžaduje žiadne ďalšie počítače. Červ skenuje priamo z PLC v sieti nové ciele, ktoré následne napadá a replikuje sa na nájdené ciele, pričom sa pôvodný hlavný program bežiaci na PLC nezmení – viac v literatúre [30].

Vedci z Gruzínskeho technologického inštitútu predstavili LogicLocker aby poskytli obrancom ICS sieti predstavu o tom, ako môžu vyzerať budúce útoky. Hlavným cieľom LogicLockeru je uzamknutie riadiaceho programu PLC vynúteným novým heslom, čo bráni legitímnym používateľom manipulovať zo zariadením. Ďalším cieľom je zašifrovanie rebríkovej logiky zo vzdialeného miesta a následne obeť vydierať. Ak obeť nesúhlasí s podmienkami útočníka, útočník môže meniť kontrolovaný proces manipuláciou rebríkovej logiky – viac v literatúre [31].

Stuxnet

Stuxnet je škodlivý počítačový červ, ktorý bol objavený v roku 2010 bieloruskou firmou VirusBlokAda. Stuxnet sa zameriava na PLC v SCADA systémoch a je zodpovedný za spôsobenie značných škôd v jadrovom programe Iránu.

Jedna vec, ktorá odlišuje Stuxnet od bežnejšieho škodlivého softvéru je to, že jeho tvorcovia doň začlenili množstvo funkcií. Tie siahajú od využívania viacerých chýb nulového dňa, úprav systémových knižníc, útok na ovládací softvér Step7 a spustenia RPC servera až po inštaláciu podpísaných ovládačov v operačných systémoch Windows.

Stuxnet sa šíri prostredníctvom niekoľkých vektorov, ktoré sú vybrané tak, aby mu umožnili infikovať PLC, na ktoré sa zameriava. Je schopný automatickej aktualizácie, aby mohol aktualizovať svoje staré verzie na novšie aj v lokálnej sieti. Komunikuje s veliteľskými a riadiacimi servermi, aby poskytoval informácie o jeho šírení a tiež je to ďalší spôsob, ako sa môže aktualizovať. Skrýva svoju prítomnosť a zdroj deštruktívnych účinkov pred zamestnancami závodu.

PLC sú pripojené k počítačom, ktoré ich riadia a monitorujú, zvyčajne nie sú pripojené k internetu. Hlavným vektorom šírenia je preto USB flash disk. Ďalšie vektory sa šíria pomocou systému Siemens WinCC, zdieľaných priečinkov Windows pre propagáciu v lokálnej sieti a cez Step 7 projekty.

Samostatný útok Stuxnet prebieha v šiestich krokoch. V prvom kroku je počítač so systémom Microsoft Windows infikovaný pomocou niektorého vektora šírenia. Pomocou digitálneho certifikátu, ktorý dokazuje, že pochádza od spoľahlivej spoločnosti, je schopný vyhnúť sa automatizovaným detekčným systémom. V druhom kroku Stuxnet skontroluje či je dané zariadenie súčasťou priemyselného riadiaceho systému so zariadeniami od spoločnosti Siemens. Takéto systémy sú v Iráne nasadené na prevádzkovanie vysokorýchlostných odstrediviek, ktoré pomáhajú obohacovať jadrové palivo. Ak je systém cieľom útoku, tak v treťom kroku sa červ pokúsi získať prístup na internet a stiahnuť si novšiu verziu alebo odovzdať informácie o ďalšom infikovanom zariadení. Ak systém nie je cieľom, Stuxnet neurobí nič. Vo štvrtom kroku červ kompromituje PLC cieľového systému za pomoci zraniteľností nulového dňa. Na začiatku piateho kroku Stuxnet sleduje operácie cieľového systému. Následne použije zhromaždené informácie na prevzatie kontroly nad PLC zariadením. V poslednom šiestom kroku Stuxnet posiela zlé príkazy do PLC zariadenia a poskytuje falošnú spätnú väzbu externým kontrolórom, čím zaisťuje nevedomosť o nesprávnom chode systému, kým nie je neskoro.

Od prvého odhalenia Stuxnet útoku bol tento červ modifikovaný a rozšíril sa do ďalších priemyselných a energetických zariadení. Stuxnet do dnešného dňa patrí medzi vysoko rizikové útoky [28, 32].

Duqu

V roku 2011 bol odhalený malvér Duqu, ktorý vykazoval podobnosti so známym červom Stuxnet. Podobne ako Stuxnet útočil na priemyselné zariadenia a dokázal sa skrývať pred bežnými antivírusovými programami, avšak s tým rozdielom, že išlo o rootkit informačného zlodeja. Duqu bolo z toho dôvodu isto možné prekonfigurovať na diaľku z riadiaceho servera tak, aby obsahoval prakticky akýkoľvek druh funkcií. Duqu 2.0 bol objavený 4 roky po prvej verzii a vychádzal z pôvodného Duqu malvéru, ktorý tak isto využíval zraniteľnosti nulového dňa [33].

Ukraine Power Grid

V roku 2015 prerušil kybernetický útok dodávku elektrickej energie pre takmer štvrť milióna Ukrajincov. Jednalo sa o prvý úspešný útok na infraštruktúru elektrickej energie v západnej časti Ukrajiny. Útočníci prerušili napájanie na 30 rozvodniach, ktoré boli mimo prevádzky až 6 hodín. SCADA zariadenia boli vyradené z prevádzkyschopného stavu a obnova napájania sa musela dokončiť manuálne. Vyšetrovaním sa zistilo, že útočníci uskutočnili výpadok pomocou BlackEnergy malvéru, ktorý patrí medzi DDoS útoky.

Rok po prvom útoku prišiel druhý útok, keď prišlo o dodávku elektrickej energie rovnaký počet ľudí. V tomto prípade bol útok sofistikovanejší a bol použitý Industroyer malvér (taktiež označovaný ako CrashOverride) [34].

Kemuri

V roku 2016 spoločnosť Verizon Security Solution uviedla, že anonymná vodná spoločnosť zažila kybernetický útok na svoju ICS sieť. Podľa spoločnosti Verizon získali útočníci prístup k aplikácii na chemické spracovanie vody, ktorá riadila ventily a prietoky pomocou stoviek PLC zariadení. Následne sa im podarilo manipulovať so systémom tak, aby sa zmenilo množstvo chemikálií vstupujúcich do prívodu vody, čím ovplyvnili možnosti úpravy a výroby vody. Aj keď útok Kemuri nemal katastrofické následky, ľahko mohol byť kritickejší, ak útočníci mali o niečo viac času a znalostí o systémoch SCADA. Kľúčovým prínosom tohoto útoku je používanie ICS siete s prístupom na internet, čo môže ohroziť kritickú infraštruktúru [34].

1.6.2 Bezpečnostné riešenia PLC zariadení

Poprední dodávatelia PLC zariadení ponúkajú bezpečnostné riešenia zamerané na široké oblasti, ako sú napríklad fyzická ochrana, deaktivácia nepoužívaných funkcií, ochrana komunikácie, systému, integrity a autorizácia a kontrola prístupu. Pri návrhoch ICS systémov by mali byť tieto oblasti brané do úvahy, mali by byť zahrnuté

v týchto systémoch a výrobcovia PLC radičov by mali tieto oblasti zakomponovať do zariadení [25]. V následujúcich podkapitolách sú jednotlivé oblasti podrobnejšie popísané.

Fyzická ochrana

Samostatná fyzická ochrana má odradiť útočníkov od manipulácie s prepínačom režimu PLC, vstupnými a výstupnými modulmi alebo pamäťovou kartou. Niektoré PLC obsahujú kryt na malý visiaci zámok alebo samostatný kryt na kľúč, ktorý musí byť otvorený pre prístup k týmto komponentom. Táto účinnosť zabezpečenia je diskutabilná v prípade, že je ho možné ľahko narušiť, preto by sa mali PLC umiestňovať do miestností s obmedzeným prístupom iba pre vybraných zamestnancov.

Deaktivácia nepoužívaných funkcií

Jedným z najzákladnejších bezpečnostných mechanizmov je odstránenie vektora útoku pre služby, ktoré sa nepoužívajú. Niektoré PLC ponúkajú možnosť deaktivovať fyzické porty, sieťové služby a dokonca aj jednotlivé príkazy. Toto všetko pomáha znižovať vektor útoku, a preto by sa mali nepoužívané funkcie vždy zakázať. Existujú aj PLC, ktoré poskytujú jemnejšiu granularitu deaktivácie, ako napríklad možnosť vypnúť všetky požiadavky na zápis.

Ochrana komunikácie

Komunikačná ochrana ponúkaná PLC siaha od jednoduchých prostriedkov, ako je zabudovaný firewall v podobe umožnenia selektívneho povolenia prenosu na základe vopred určeného zoznamu IP adries až po SSL alebo TLS protokoly. Pri použití IP whitelistu sa dá použiť nástroj na falšovanie IP adries a toto zabezpečenie sa dá ľahko obísť, preto je lepšie používať šifrovacie protokoly ako je SSL alebo TLS. Ďalšou možnosťou, ktorú PLC ponúkajú je protokol HTTPS. Nejde však o najbezpečnejšie riešenie, pretože sa dá na PLC útočiť pomocou známych zraniteľností tohoto protokolu. Poslednou a najbezpečnejšou možnosťou komunikácie s PLC je za pomoci použitia externých modulov, ako sú externé brány firewall a VPN, ktoré možno použiť s PLC na zaistenie zvýšenej bezpečnosti.

Ochrana systému

Predajcovia PLC si uvedomujú potrebu zabudovania robustnosti svojho produktu proti útokom DoS a DDoS. Niektoré PLC si v tejto oblasti nárokujú robustnosť a jestvujú aj certifikované autority, ako napríklad ISASecure[1], ktoré certifikujú testy

[1] https://www.isasecure.org/en-US/

v týchto oblastiach. Existujú PLC, ktoré monitorujú frekvenciu neobvyklých činností a prijímajú príslušné opatrenia. To však nie je také výkonné alebo pokročilé ako samostatný systém detekcie vniknutia (Intrusion Detection Systems – IDS) alebo systém prevencie narušenia (Intrusion Prevention Systems – IPS) používaný v IT priemysle, a preto by tieto systémy mali byť zabudované v ICS sieťach.

Ochrana integrity

Ochranu integrity možno rozdeliť do troch hlavných oblastí. Prvá oblasť je statický obraz firmvéru PLC. Tento obraz sa používa na obsluhu PLC, podobne ako BIOS počítača. Druhou oblasťou je konfigurácia, ktorá je navrhnutá používateľom pomocou softvéru na programovanie PLC a je nahraná do PLC na riadenie jeho automatizačného systému. Tretia oblasť sa týka operatívneho spustenia užívateľského programu; v tom prípade sa hodnoty údajov sa dynamicky načítajú a zapisujú do nich, v podstate sa menia tak, aby odrážali stav činnosti automatizovaného systému.

Integrita obrazu firmvéru PLC je riešená pomocou technológie digitálneho podpisu, čo poskytuje dôveru v integritu a autenticitu obrazu. Pre overenie integrity firmvéru existujú aj nástroje; Mcminn a kolektív predstavili nástroj v systémoch SCADA (viac v literáture [35]) a Garcia navrhol nástroj s analytickou technikou (viac v literatúre [36])

Ochrana konfigurácie používateľa pred škodlivými zmenami je zložitejšia. Ak je možné oprávnením používateľom obmedziť stiahnutie konfigurácie , stačí algoritmus hash. Avšak v niektorých scenároch, kde môže byť konfigurácia dynamická neexistuje dobrý mechanizmus na zabezpečenie autorizácie používateľa a niektoré PLC to riešia poskytnutím spôsobu detekcie a hlásia tieto zmeny. Toto však skôr zabezpečuje detekciu ako ochranu integrity.

Tretiu oblasť hodnôt dynamických údajov nemožno ľahko vyriešiť, pokiaľ sa na prenos týchto zmien nepoužije zabezpečený komunikačný mechanizmus, preto by sa mali na prenos používať mechanizmy, ktoré boli spomenuté pri ochrane komunikácie.

Autorizácia a kontrola prístupu

PLC ponúkajú rôzne autorizácie a riadenia prístupu pre rôzne oblasti, ako sú konfiguračné a runtime dáta. Tieto oblasti je možné ďalej segregovať na základe prístupového média, ako je napríklad fyzické rozhranie, komunikačný protokol a typ príkazu. Napríklad môžu existovať úrovne prístupu None, Read alebo Read/Write pre konfiguráciu z vnútornej siete a pre externú sieť. Niektoré PLC poskytujú riadiaci prístup k jednotlivým príkazom odosielaným do PLC, ak to protokol podporuje. Autorizácia a riadenie prístupu sa zvyčajne realizujú pomocou mechanizmu hesla na udelenie

prístupu. Väčšina z týchto mechanizmov má obmedzenia z dôvodu nedostatku bezpečnosti protokolu. V niektorých prípadoch sa používa čistý text, zatiaľ čo v iných prípadoch neexistuje autorizovaný komunikačný kanál.

1.7 Protokoly prevádzkových technológii

Priemyselné sieťové protokoly je možné rozdeliť do dvoch hlavných kategórii, a to protokoly prevádzkovej zbernice a backend protokoly. Na pripojenie prevádzkových zariadení k radičom, ako je napríklad PLC sú potrebné protokoly prevádzkovej zbernice, ako sú Modbus TCP, Ethernet/IP, DNP3 a mnoho ďalších. Protokoly typu backend sú potrebné najmä na priame prepojenie niekoľkých priemyselných závodov alebo riadiacich centier. Priemyselné protokoly boli vyvinuté z originálnych proprietárnych protokolov, ktoré sú kompatibilné s bežnými sieťovými protokolmi a štandardmi, ako je internetový protokol (IP) alebo ethernet. Samostatné protokoly sú určené na efektívnosť a spoľahlivosť, a preto mnoho protokolov používa kontrolné súčty, čo ale poskytuje nedostatočnú ochranu pred kybernetickými útokmi, v prípade spoľahlivosti musia totiž spĺňať tvrdé požiadavky v reálnom čase. Pretože protokoly sú tiež navrhnuté tak, aby boli efektívne, sú všetky ďalšie funkcie alebo vlastnosti vynechané alebo zanedbané, aby sa zabezpečila čo najmenšia hlavička protokolu. Najbežnejšie protokoly OT siete sú vypísané v tabuľke 1.2.

Protokol	**Porty**	**Protokol**	**Porty**
ICCP	102	Hart-IP	5094
Siemens S7	102	CoAP	5683, 5684
Modbus	502, 802	Emerson ecmp	6160
Red Lion	789	OMRON FINS	9600
Foundation Fieldbus	1089, 1090, 1091, 3622	Johnson Controls	11001
PCWorx	1962	Zigbee	17754 až 17756
Niagara Fox	1911, 4911	GE-SRTP	18245, 18246
Ethernet/IP	2036, 2221, 2222, 44818	DNP3	19999, 20000
IEC 60870-5-104	2404, 19998	ProConOS	20547
CODESYS	2455	PROFINET	34962 až 34964
Emerson ROC	4000	EtherCAT	34980
OPC UA	4840, 4843	BACnet	47808
MELSEC-Q	5006, 5007	FL-net	55000 až 55003

Tab. 1.2: Tabuľka najbežnejších OT protokolov.

Najpoužívanejšie priemyselné Ethernetové protokoly podľa prieskumu HMS [37] a ďalšie protokoly, ktoré sa používajú s PLC zariadeniami sú popísané podrobnejšie v následujúcich podkapitolách.

Modbus

Modbus protokol bol pôvodne vyvinutý spoločnosťou Modicon v roku 1979. Jedná sa o otvorený štandard pre priemyselné výrobné prostredie, ktorý je široko používaný a podporovaný mnohými výrobcami priemyselných komponentov. V súčasnosti je Modbus pod správou organizácie Modbus [38]. Protokol Modbus je založený na komunikačnej štruktúre klient-server na dopytovanie a odosielanie údajov z PLC (server) do zariadení ako server MTU alebo SCADA (klient). Tento princíp sa často označuje aj ako master/slave komunikácia. Transakcie údajov iniciuje iba server a sú buď typu dotaz/odpoveď, kde je adresovaný iba jeden klient, alebo typu broadcast/žiadna odpoveď, kde sú adresovaní všetci klienti. Transakcia obsahuje jeden dotaz a jeden rámec odozvy alebo jeden vysielací rámec [39].

Modbus sa pôvodne používal cez sériovú zbernicu (RS-232, RS-422, RS-485 atď.) a časom sa adaptoval, aby bolo možné komunikovať po sieťach založených na TCP/IP. V súčastnosti existuje viac typov Modbus protokolov a tie najpoužívanejšie sú [40]:

- **Modbus RTU** – sériový binárny komunikačný protokol, ktorý primárne využíva na komunikáciu sériové rozhranie RS–232 alebo RS–485. Ide o všeobecne akceptovaný protokol vďaka ľahkému použitiu a spoľahlivosti a je podporovaný takmer každým komerčným SCADA,HMI, OPC serverom a softvérovým programom na zber dát na trhu. Jedná sa o protokol typu 1Master x nSlaves, kedy slave zariadení môže byť maximálne 254. Modbus RTU je široko používaný v systémoch riadenia budov a priemyselnej automatizácie.
- **Modbus ASCII** – sériový komunikačný protokol ASCII je podobný ako protokol Modbus RTU, ale binárny obsah sa transformuje na bežné znaky ASCII. Tento protokol sa nepoužíva tak často ako Modbus RTU.
- **Modbus TCP/IP** – sieťový protokol, ktorý využíva TCP/IP s rozhraním Ethernet. Princíp komunikácie je rovnaký ako pri Modbus RTU protokole a zariadenia komunikujú cez port 502.
- **Modbus PLUS** – proprietarný protokol firmy Schneider Electric typu peer-to-peer založený na komunikácii odovzdávajúcej tokeny. Prenosová rýchlosť protokolu je 1 Mb/s, podporuje maximálne 64 staníc, PC stanica potrebuje špeciálnu hardvérovú sieťovú kartu v sieti a je potrebné používať špeciálnu kabeláž a komponenty [41].

- **Modbus/TCP Security** – protokol poskytuje ochranu kombináciou protokolu Transport Layer Security (TLS) s protokolom Modbus. TLS zapuzdruje pakety Modbus na zabezpečenie autentifikácie a ochrany integrity správ. Tento protokol taktiež využíva digitálne certifikáty X.509v3 na autentizáciu servera a klienta. Modbus Security využivá port 802.

Siemens S7

Protokol Siemens S7 je proprietárny protokol spoločnosti Siemens, ktorý bol uvedený do prevádzky spolu s predstavením produktovej rady Simatic S7 v roku 1994. Používa sa na programovanie PLC, výmenu údajov medzi PLC, prístup k PLC údajom zo systému SCADA a na diagnostické účely. Protokol S7 využíva rozhranie Ethernet a komunikuje cez port 102. V prípade PLC alebo doplnkových komunikačných moduloch je možné použiť konektor PROFINET na komunikáciu pomocou protokolu S7. V prípade, že Siemens PLC nedisponuje PROFINET konektorom je možná komunikácia za pomoci prídavného prevodníka alebo modulu Ethernet. V súčastnosti existuje už aj protokol S7 plus, ktorý je tak isto proprietárny protokol spoločnosti Siemens. S7 plus poskytuje rôzne ochrany integrity a výmeny kľúčov, ktoré závisia od verzie protokolu a zariadenia s ktorým sa komunikuje. Pri komunikácii s PLC S7-1500 a verzii protokolu 2 je využívaná ochrana integrity jednotlivých správ jednoduchou výmenou kľúčov. Komunikácia pomocou verzie 3 s rovnakým PLC zariadením používa ochranu integrity jednotlivých fragmentov s výmenou kľúča kryptografickej výzvy a odpovede pre každú reláciu. Protokol S7 plus sa používa na rovnaké účeli ako starší protokol S7 [42, 43].

PROFINET

PROFINET je moderný koncept štandardov distribuovanej automatizácie. Prvé PROFINET špecifikácie boli zverejnené v roku 2002 a za jeho vznikom stojí organizácia PI North America. Je založený na Ethernete a integruje existujúce systémy priemyselnej zbernice, najmä PROFIBUS, jednoducho a bez zmeny. Toto riešenie je schopné pracovať v zložitých priemyselných prostrediach a je schopné dodať rýchlosť a presnosť požadovanú výrobnými procesmi. Jedná sa o komunikačný protokol, ktorý slúži na výmenu údajov medzi radičmi a zariadeniami. Pre komunikáciu pomocou PROFINET protokolu sú rezervované porty 34962 až 34964. Vďaka modulárnej škále funkcií je flexibilným riešením pre všetky aplikácie a trhy. Prostredníctvom PROFINET možno implementovať aplikácie pre automatizáciu výroby a procesov, bezpečnostné aplikácie a celú škálu pohonnej techniky až po izochrónne aplikácie na riadenie pohybu [44].

Ethernet/IP

Ethernet/IP je produktom vývoja konzorcia výrobcov a organizácií združených v asociáciách ODVA (Open DeviceNet Vendor Association) a ControlNet International na čele s firmou Rockwell Automation. Prvýkrát bol predstavený v roku 2001. Protokol je plne kompatibilný so štandardom Ethernet a pracuje na portoch 2036, 2221, 2222 a 44818. V rámci siete Ethernet/IP sú jednotlivým ethernetovým uzlom priradené vopred definované typy zariadení so špecifickými vlastnosťami a funkciami, takzvané profily. Profily zariadení a aplikačná vrstva Ethernet/IP sú tvorené protokolom CIP. Protokol umožňuje prenos základných vstupných a výstupných údajov, nahrávanie a sťahovanie nadstavených hodnôt a programov, ale aj monitorovanie [45].

EtherCAT

Štandard priemyslového Ethernetu EtherCAT bol vyvinutý s dôrazom na rýchly prenos dát s krátkym komunikačným cyklom. Vývoj a propagáciu mala na starosť spoločnosť Beckhoff Automation, ktorá predstavila protokol v roku 2003. V tom istom roku bola založená organizácia EtherCAT Technology Group, ktorá momentálne spravuje tento protokol. EtherCAT je vysoko výkonná, nízkonákladová a ľahko použiteľná technológia priemyselného ethernetu s flexibilnou topológiou. Pri vývoji bola hlavná pozornosť venovaná krátkym dobám cyklu ($\leq 100\ \mu$s), nízkym oneskoreniam pre presnú synchronizáciu ($\leq 1\ \mu$s) a nízkym nákladom na hardvér. Sieť EtherCAT používa komunikačnú schému master/slave. Dáta nie sú podriadeným zariadeniam (slave) odosielané ako jednotlivé ethernetové rámce, ale rámec prechádza behom jedného cyklu cez všetky podriadené zariadenia. Komunikovať môžu navzájom nie len podriadené zariadenia s príslušnými nadriadenými, ale aj jednotlivé master stanice, poprípade slave zariadenia. Komunikácia medzi slave zariadeniami prebieha buď v rámci jedného cyklu pokiaľ adresát leží po smere alebo pomocou dvoch cyklov cez master zariadenie. Pre EtherCAT protokol je rezervovaný port 34980 a je zameraný predovšetkým na použitie v strojárenstve pri riadení pohonov [46].

OPC UA

OPC UA je ďalšia generácia technológie OPC, ktorú spravuje OPC Foundation. OPC UA je bezpečnejší, otvorenejší a spoľahlivejší mechanizmus na prenos informácií medzi servermi a klientmi. Poskytuje viac otvorených transportov, lepšiu bezpečnosť a úplnejší informačný model ako starý štandard OPC, ktorý sa volá OPC Classic. Hlavným cieľom OPC UA je nezávislosť a interoperabilita na platforme. Technicky bol štandard postavený na základe základných webových technológií (TCP/IP, http/SOAP), kde základné koncepcie výmeny údajov boli prijaté, kombinované a doplnené ďalšími koncepciami. Pre komunikáciu pomocou tohto protokolu

sú vyhradené porty 4840 a 4843. OPC UA poskytuje veľmi flexibilný a prispôsobivý mechanizmus na presun údajov medzi systémami podnikového typu a druhmi ovládacích prvkov, monitorovacích zariadení a senzorov, ktoré interagujú s údajmi v reálnom svete. Vďaka tomu dokáže pomocou OPC UA komunikovať aj najmenší dedikovaný radič s komplexnými serverovými aplikáciami. Pomocou OPC UA je možné posielať informácie od jednoduchého výpadku až po obrovské množstvo vysoko komplexných informácii o celej prevádzke [47].

DNP3

DNP3 vyvinula spoločnosť GE Harris. Prvá verzia protokolu bola zverejnená v roku 1993, v tom istom roku bola zodpovednosť za definovanie ďalších špecifikácii DNP3 a vlastníctvo špecifikácii prenesená na DNP Users Group. DNP3 je založený na objektovom modeli redukujúcom bitové mapovanie dát, ktoré vyžadujú iné menej objektovo orientované protokoly. Znižuje nerovnosť paradigiem monitorovania a kontroly stavov, ktoré sa zvyčajne nachádzajú v protokoloch, ktoré neposkytujú takmer žiadne vopred definované objekty. Vývoj DNP3 bol komplexným úsilím o dosiahnutie otvorenej interoperability založenej na štandardoch medzi počítačmi rozvodne, RTU, IED a hlavnými stanicami pre priemysel elektrických rozvodov. Najčastejšie sa používa v SCADA systémoch a od jeho vzniku sa protokol začal široko využívať v priemyselných odvetviach ako voda, odpadová voda, doprava, ropný a plynárenský priemysel. DNP3 protokol pre komunikáciu medzi zariadeniami využíva porty 19999 a 20000 [48].

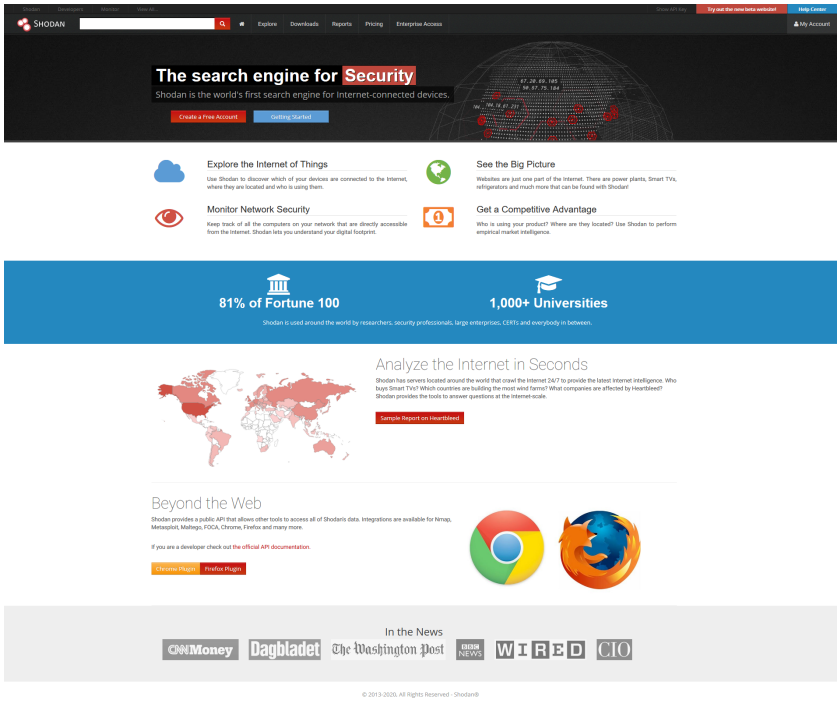
2 Vyhľadávacie nástroje zariadení

Vyhľadávacie nástroje ako Google, Yahoo alebo Microsoft bing sú jedny z hlavných mechanizmov, pomocou ktorých používatelia získavajú informácie na internete. Vďaka týmto vyhľadávačom vedia používatelia vyhľadať bežné informácie ako webové stránky, obrázky, videá a iné. Existujú však aj vyhľadávacie nástroje zariadení, ako napríklad Shodan, Censys, ZoomEye a BinaryEdge, ktoré na rozdiel od bežných vyhľadávačov zhromažďujú informácie o zariadeniach pripojených k internetu.

V nasledujúcich podkapitolách (2.1, 2.2, 2.3, 2.4) sú popísané jednotlivé vyhľadávacie nástroje zariadení, ktoré boli porovnané v rámci praktickej časti.

2.1 Shodan

Prvý vyhľadávací nástroj zariadení bol Shodan. Za jeho vznikom stojí programátor John Matherly, ktorý prišiel s touto myšlienkou v roku 2003. Samostatný Shodan pre bežných užívateľov prišiel v roku 2009 spolu s webovým užívateľským rozhraním (obrázok 2.1) a je dostupný na webovej stránke https://www.shodan.io/. Okrem webového rozhrania je možné pristupovať k dátam pomocou rozhrania príkazového riadku (Command Line Interface – CLI) alebo programovacieho rozhrania softvérovej aplikácie (Application programming interface – API) [49, 50].



Obr. 2.1: Úvodná stránka Shodan vyhľadávača.

Pôvodne vedel vyhľadávať zariadenia s IPv4 adresami a pracoval so základnými portami 21(FTP), 22(SSH), 23(Telnet) a 80(HTTP) [51], v momentálnej dobe zisťuje informácie za pomoci viac ako sto portov (zoznam portov nájdete v literatúre [50]). Od októbra 2015 začal Shodan mesačne zhromažďovať milióny banerov zo zariadení, ktoré sú k internetu pripojené pomocou IPv6 adries.

Základnou jednotkou algoritmov zhromažďovania údajov, ktoré Shodan využíva, je baner. Baner je textová informácia, ktorá popisuje služby v zariadení. Obsah banera sa líši v závislosti od typu služby. Ako rozdielne banery môžu vyzerať si môžete pozrieť obrázok 2.2, kde sa na ľavej strane nachádza typický HTTP baner a na pravej strane baner priemyselného protokolu Siemens S7, z ktorého vieme vyčítať, že sa jedná o PLC zariadenie.

```
HTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 14 Oct 2020 15:24:30 GMT
Content-Type: text/html
Content-Length: 564
Connection: keep-alive
```

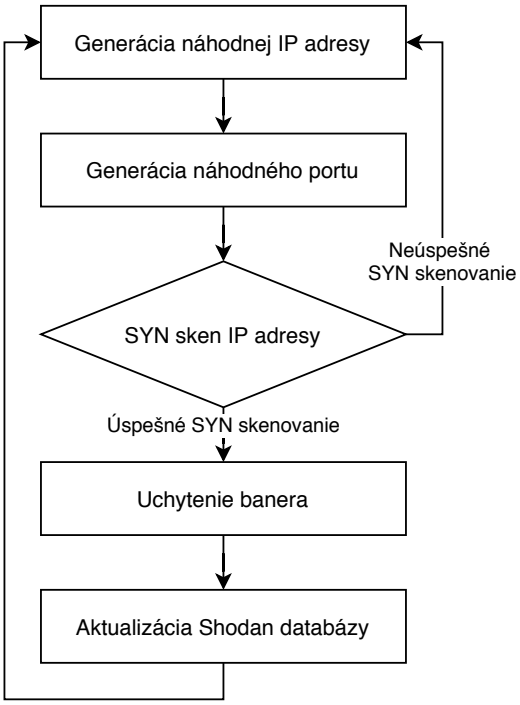
```
Copyright: Original Siemens Equipment
PLC name: S7300/ET200M station_1
Module type: CPU 314C-2 DP
Unknown (129): Boot Loader          A
Module: 6ES7 314-6CG03-0AB0  v.0.1
Basic Firmware: v.2.6.11
Module name: PLC_1
Serial number of module: S C-UDA155062006
Plant identification:
Basic Hardware: 6ES7 314-6CG03-0AB0  v.0.1
```

Obr. 2.2: HTTP baner (vľavo), Siemens S7 baner (vpravo).

Okrem banera Shodan získava aj metadáta o zariadeniach ako sú jeho geografické umiestnenie, názov hostiteľa, operačný systém, poskytovateľ internetového pripojenia (Internet service provider – ISP) a ďalšie. Väčšinu z nich možno vyhľadať cez webové rozhranie, niektoré údaje sú k dispozícii iba prostredníctvom API [50].

Pri posielaní vyhľadávacieho dotazu, ktorý obsahuje iba text, napríklad „Google“ Shodan implicitne prehľadáva text hlavného baneru, čo znamená, že Shodan nám zobrazí iba výsledky, pri ktorých sa v baneri zobrazil text „Google“. Pre prehľadávanie metadát musíme použiť filtre; ak chceme vyhľadať IP adresy, ktoré patria spoločnosti Google, musíme použiť filter a zadať vyhľadávací parameter ako **org:"Google"** (zoznam filtrov nájdete v literatúre [50]).

Shodan pri prehľadávaní internetu indexuje zariadenia a zisťuje dostupné služby pomocou TCP SYN skenovania. Metóda Shodan vyhľadávania je zobrazená na obrázku 2.3. V prvom kroku sa vygeneruje náhodná IP adresa, ku ktorej sa priradí náhodný port zo zoznamu portov, ktoré Shodan podporuje. Na danú IP adresu a port sa následne odošle TCP paket s nadstaveným príznakom SYN. Ak sa z cieľového portu danej IP adresy vráti odpoveď s príznakom SYN/ACK, jedná sa o otvorený port, v tomto prípade sa vykoná uchytenie banera. Uchytenie banera je technika používaná na získavanie informácii o systéme zariadenia v sieti a službe bežiacej na



Obr. 2.3: Shodan vyhľadávacia metóda [52].

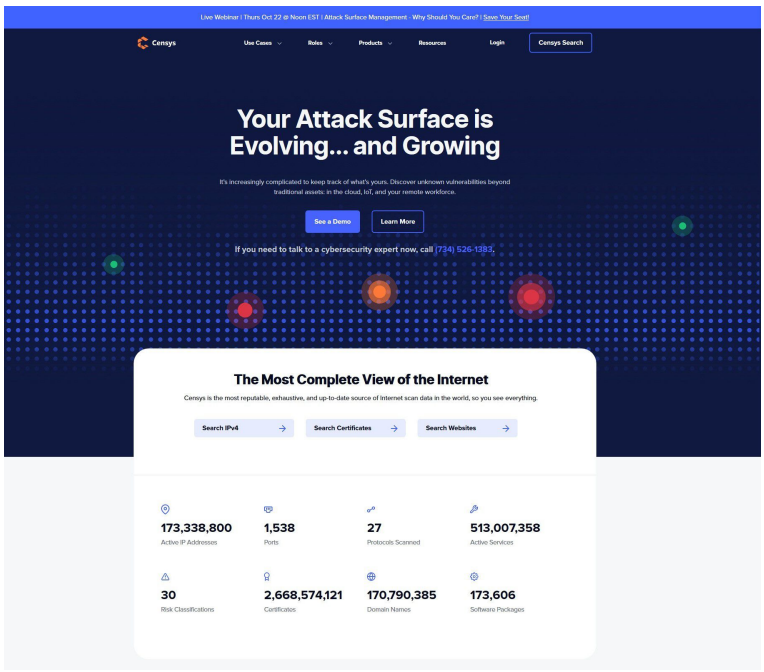
jeho otvorených portoch. Následne sa zodpovedná IP adresa zariadenia spolu s portom a servisným banerom uloží do databázy, ak sa zariadenie v databáze vyskytuje, aktualizuje informácie o danom zariadení. V prípade žiadnej alebo odpovede s príznakom RST, kedy sa jedná o uzavretý port, skenovanie pokračuje vygenerovaním novej náhodnej IP adresy a servisného portu [53].

Okrem vyhľadávania informácii o zariadení, Shodan ponúka aj:

- Shodan Maps – jedná sa o spôsob vizuálneho preskúmania výsledkov vyhľadávania, keď vieme naraz zobraziť až 1000 výsledkov. Pri oddialení alebo priblížení mapy sa vyhľadávací dotaz upraví tak, aby zobrazoval výsledky pre oblasť, na ktorú sa práve pozeráme. V mapách je taktiež možné využiť filtre pri vyhľadávaní.
- Shodan Exploits – vyhľadávač zraniteľností a exploitov, ktoré Shodan zhromažďuje z CVE (Common Vulnerabilities and Exposures), Exploit DB a Metasploit databáz.
- Shodan Images – vyhľadávač snímkov obrazoviek, ktoré Shodan zachytí pri skenovaní internetu
- Honeyscore – nástroj, ktorý vypočítava pravdepodobnosť existencie honeypotu na danej IP adresa . Tento nástroj je zatiaľ spustený ako prototyp.
- Shodan Monitor – monitorovanie určitej IP adresy alebo rozsahu siete [50]

2.2 Censys

Censys vyhľadávač bol vyvinutý ako súčasť open-source projektu na univerzite v Michigane, ktorého cieľom bola kompletná databáza všetkých zariadení pripojených na internete. Táto databáza mala pomôcť bezpečnostným expertom pri hodnotení bezpečnosti zariadení a služieb pripojených k internetu. Spoločnosť Censys bola založená v roku 2015, v tom istom roku bol zverejnený Censys vyhľadávač pre verejnosť s webovým užívateľským rozhraním (obrázok 2.4). Pristupovať k databáze s dátami, ktoré Censys zhromažduje je možne z webovej stránky https://censys.io/ alebo pomocou API [54, 55].



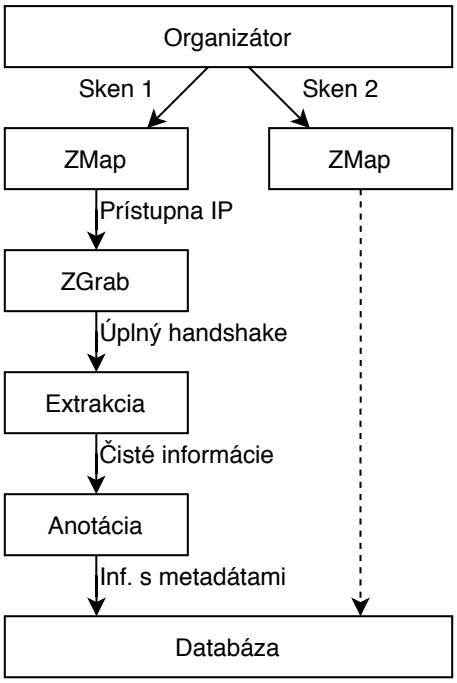
Obr. 2.4: Úvodná stránka Censys vyhľadávača.

V súčasnej dobe Censys vyhľadáva zariadenia iba s IPv4 adresami a detekuje 36 protokolov (zoznam protokolov sa nachádza v literatúre [55]) cez 2029 portov, čo umožňuje identifikáciu služieb bežiacich aj na neštandardných portoch [55].

Censys rovnako ako Shodan používa baner (obrázok 2.2) ako základnú jednotku pre zber informácii, okrem základných informácii zhromažďuje aj metadáta o zariadeniach.

Vyhľadávacia politika Censysu je nadstavená tak, že pri vyhľadávaní dotazov sa prehľadávajú banery aj metadáta; v prípade potreby prehľadávania len metadát je potrebné použiť filtre (zoznam filtrov nájdete v literatúre [55]).

Podobne ako Shodan zhromažďuje údaje o zariadeniach a webových stránkach prostredníctvom periodického a horizontálneho skenovania IPv4 adresného priestoru. Metóda zhromažďovania informácii Censys vyhľadávača je zobrazená na obrázku 2.5.



Obr. 2.5: Censys vyhľadávacia metóda [52].

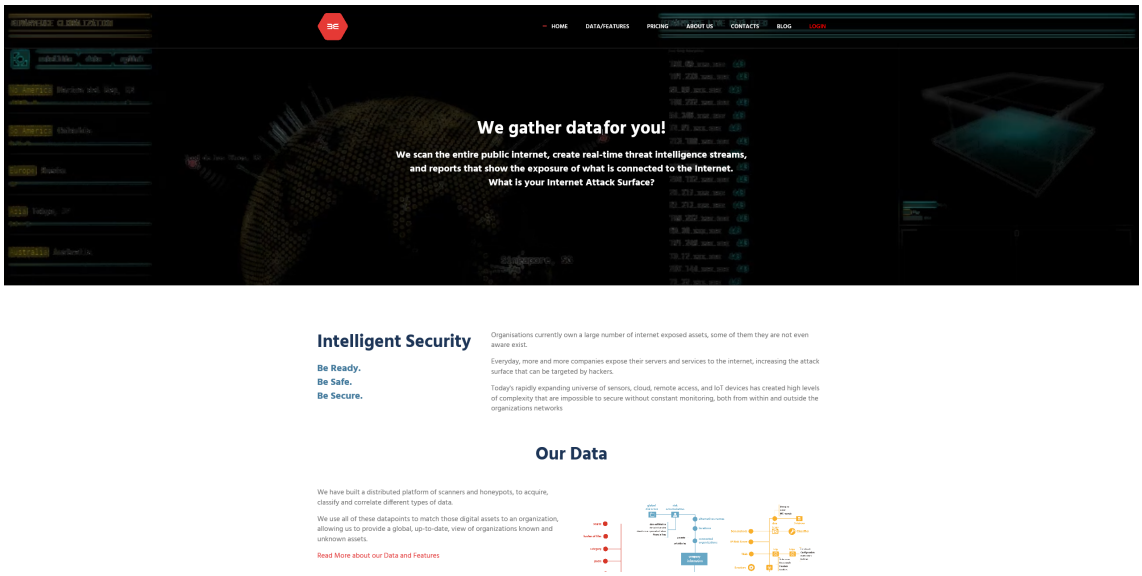
Pri tejto metóde skenovania sa používajú nástroje ZMap [56] a ZGrab [57]. ZMap najskôr pomocou TCP SYN skenovania skontroluje či je zariadenie pripojené do siete pomocou IPv4 adresy a či je port otvorený. V prípade odozvy zo zariadenia, ktorý sa má skenovať, ZGrab, skener aplikačnej vrstvy vykoná uchytenie banera a zhromaždí informácie o službe príslušného portu. Následne Censys extrahuje najdôležitejšie informácie z uchyteného banera a zhromaždených informácii. Po extrakcií dát k nim Censys pridá ďalšie metadáta a uloží ich do databázy, v prípade výskytu záznamu o zariadení iba aktualizuje informácie [57].

Censys podporuje aj vyhľadávanie certifikátov X.509 s verejnými kľúčmi a zhromažďuje najnavštevovanejšie web stránky z databázy Alexa Top 1 Million [55].

2.3 BinaryEdge

Vyhľadávač vznikol v roku 2015 pod názvom 40fy a neskôr bol premenovaný na BinaryEdge. Za jeho vznikom a prevádzkou stojí firma BinaryEdge so sídlom v Zürichu vo Švajčiarsku. Firma sa zameriava na získavanie, analýzu a klasifikáciu údajov z internetu pomocou práce v oblasti kybernetickej bezpečnosti, dátovej vedy a strojového učenia. BinaryEdge dáta sú dostupné pomocou užívateľského webového rozhrania (obrázok 2.6) na URL adrese https://www.binaryedge.io/ alebo pomocou API [58].

BinaryEdge sa primárne zameriava na organizácie, neustále zhromažďuje a koreluje údaje zo zariadení prístupných na internete pomocou IPv4 a IPv6 adries, čo



Obr. 2.6: Úvodná stránka BinaryEdge vyhľadávača.

im umožňuje vidieť ich počítačovú sieť a informácie, ktoré vystavujú útočníkom. Umožňuje zobrazovať ich známe a neznáme zraniteľnosti na základe mapovania digitálnych aktív organizácie, a to hlavne:

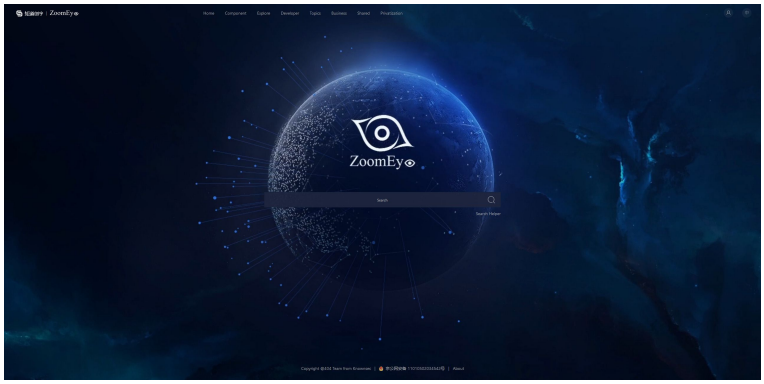
- Porty a služby
- Možné zraniteľnosti
- Prístupné vzdialené pracovné plochy
- Neplatné SSL certifikáty
- Nesprávne nakonfigurované zdieľania v sieti
- Databázy

Na odhaľovanie zraniteľností získava BinaryEdge informácie z úložiska NVD (National Vulnerability Database). NVD je americké vládne úložisko zraniteľností predstavovaných pomocou protokolu SCAP (Security Content Automation Protocol). Na analýzu zraniteľností sa používajú údaje CVE a CVSS z úložiska NVD. Pre každú IP adresu, na ktorej bol nájdený otvorený port s bežiacou službou sa vyhľadajú všetky CVE pre daný produkt a verziu. Následne sa vyčísli závažnosť zraniteľnosti pomocou CVSS.

BinaryEdge má aj vlastnú distribuovanú sieť honeypotov. Honeypot je informačný systém, ktorého cieľom je priťahovať potenciálnych útočníkov a zaznamenávať ich činnosť. Tiež poskytuje plne automatizovaný systémom detekcie anomálií, ktorý umožňuje v reálnom čase detegovať, kedy v určitých cieľových portoch, IP adresách alebo krajinách dôjde k výkyvom. Torrent a DHT (Distributed hash table) monitorovanie, ktoré vďaka globálne rozmiestneným poslucháčom dokáže zistiť a informovať či sa v danom sieťovom priestore zdieľajú alebo sťahujú torrenty [58, 59].

2.4 ZoomEye

ZoomEye je prvý čínsky vyhľadávač, ktorý v Číne nesie pomenovanie Zhong Kui's Eye. Za jeho vývoj a prevázku zodpovedá tím 404 Laboratory z firmy Knowsec. Dáta z vyhľadávača sú dostupné pomocou webového užívateľského rozhrania (obrázok 2.7) z URL odkazu https://www.zoomeye.org/ alebo pomocou API [60].



Obr. 2.7: Úvodná stránka ZoomEye vyhľadávača.

ZoomEye dokáže vyhľadávať zariadenia s IPv4 a Ipv6 adresami a skenovať ich služobné porty a protokoly. Okrem vyhľadávania zariadení je schopný prehľadávať aj webové stránky a odhaľovať ich zraniteľnosti. Ako jadro na získavanie údajov sa používajú nástroje XMap a WMap. Pre vyhľadávanie zariadení sa používa integrácia týchto nástrojov s výsledkami rozsiahleho skenovania NMap (Network Mapper). Prostredníctvom veľkého počtu globálnych vyhľadávačov zameraných na mapovanie internetu dokáže ZoomEye vyhľadávať nepretržite 24 hodín denne [61, 62].

Podrobné informácie ako ZoomEye funguje niesu k dispozícii. Knowsec nezverejnil dokumentáciu a väčšina URL odkazov na https://www.zoomeye.org/ je presmerovaných na webové stránky v čínskom jazyku.

3 Porovnanie vyhľadávacích nástrojov pomocou webového rozhrania

V tejto kapitole je popísané porovnanie vyhľadávacích nástrojov zariadení, ktoré boli popísané v kapitole 2. Porovnávanie vyhľadávačov je zamerané na priemyselné siete a PLC zariadenia.

3.1 Porovnanie vyhľadávačov

Táto podkapitola sa zaoberá porovnávaním vyhľadávačov na základe informácií na webovej stránke a dostupnej dokumentácie jednotlivých vyhľadávačov. Porovnané boli IP adresy, ktoré sú jednotlivé vyhľadávače schopné skenovať, ďalej ako je možné k dátam pristupovať a protokoly a porty, ktoré dokážu jednotlivé vyhľadávače skenovať. Okrem porovnania sú popísané aj základné informácie jednotlivých vyhľadávačov, ako je rok založenia, URL odkaz, z ktorého sú jednotlivé vyhľadávače dostupné, aké nástroje na vyhľadávanie používajú a či disponujú honeypotmi. Všetky zistené informácie sú podrobnejšie popísané nižšie a sú vhodné pre nových užívateľov, ktorí chcú skenovať alebo vyhľadať ICS zariadenia. Dané údaje sa nachádzajú aj v tabuľke A.1.

Pri porovnávaní vyhľadávania na základe IP adresy sa zistilo, že vyhľadávače Shodan, BinaryEdge a ZoomEye sú schopné vyhľadať zariadenia, ktoré sú pripojené do verejnej siete pomocou IPv4 alebo IPv6 adresy. Vyhľadávač Censys ako jediný nedokáže nájsť zariadenia, ktoré využívajú IPv6 adresu.

Nástroje vyhľadávania sú v tabuľke vypísané z informačného dôvodu a sú tam aj napriek tomu, že z týchto údajov nedokážeme vo vyhodnotení určiť, ktorý vyhľadávač je lepší. Vyhodnotenie efektívnosti týchto nástrojov je možné určiť až z porovnania výsledkov vyhľadávania, ktoré je vykonané v podkapitole 3.2.

Z hľadiska prístupu k dátam vieme určiť, že vyhľadávač Shodan má najviac možností ako k samostatným dátam pristupovať. Shodan dokáže pristupovať k dátam pomocou webového rozhrania, CLI a API, pričom ostatné vyhľadávače majú možnosť prístupu len pomocou webového rozhrania a API. Výhodou CLI je to, že k dátam z vyhľadávačov sa dá pristupovať aj z operačných systémov bez GUI.

Pri porovnaní protokolov OT a ich portov vieme určiť, že najvhodnejší vyhľadávač OT systémov a ich zariadení je Shodan; druhým najlepším je ZoomEye. Shodan dokáže vyhľadávať na základe šestnástich protokolov a devätnástich portov[1], pričom ZoomEye dokáže vyhľadávať na základe štrnástich protokolov a rovnakom počte

[1] https://leanpub.com/shodan

portov[2]. Censys na vyhľadávanie využíva šesť protokolov a portov[3] a BinaryEdge tieto informácie nikde nemá uvedené. O aké protokoly a porty sa jedná je podrobne vypísané v tabuľke.

Censys je jediný vyhľadávač, ktorý disponuje aj sieťou honeypotov. Jedná sa o rozmiestnené zariadenia honeypot v sieti, vďaka ktorým je Censys schopný nalákať kybernetických útočníkov. Následne je schopný detegovať, odkloniť a študovať pokusy s cieľom získať neoprávnený prístup k informačným systémom. Shodan ponúka službu honeyscore, ktorá vie na základe IP adresy určiť či sa jedná o reálne zariadenie alebo honeypot. Tieto informácie sú v tabuľke zahrnuté z toho dôvodu, že honeypot dokáže zbierať údaje o útočníkoch a škodlivých malvéroch a na základe týchto informácii sa vedia korporácie zamerať na lepšie zabezpečenie systémov a zariadení.

3.2 Porovnanie účtov a výsledkov vyhľadávania

Táto podkapitola je zameraná na rozdiely užívateľských účtov a výsledkov vyhľadávania jednotlivých vyhľadávačov. Podkapitoly 3.2.1 až 3.2.4 sa zaoberajú rozdielmi vyhľadávania a prístupu k API pre neregistrovaných užívateľov, registrovaných užívateľov a registrovaných užívateľov s akademickým členstvom. Porovnanie bolo vykonané pomocou manuálneho vkladania a počítania dotazov a na základe dostupnej dokumentácie.

Po porovnaní jednotlivých účtov boli porovnané aj výsledky vyhľadávania, ktorým sa venuje podkapitola 3.2.5. Všetky vyhľadávania boli vykonané cez webové rozhrania jednotlivých vyhľadávačov. Na dopracovanie sa k najpresnejším výsledkom boli manuálne skúšané rôzne filtre a ich kombinácie.

3.2.1 Účet Shodan vyhľadávača

Na Shodane sa dá vyhľadávať aj bez potrebnej registrácie, pri vyhľadávaní však v dotaze nemôžu byť použité filtre, ale iba čisto text a je možné zobraziť iba prvú stránku, čo je 10 výsledkov. Pri dotaze kde sa nachádza čisto iba text, Shodan zobrazí výsledky, kde sa text z dotazu nachádza v banery.

Pri registrácii účtu Shodan je potrebné vyplniť používateľské meno, ktoré môže byť aj e-mailová adresa, heslo a e-mailovú adresu. Po zaregistrovaní príde na e-mail potvrdzujúci URL odkaz, ktorým sa účet aktivuje.

Shodan účet bol vytvorený pomocou školského e-mailu, vďaka ktorému sa užívateľ stane členom a je možné zobraziť prvých 20 strán, čo je 200 výsledkov. Pri

[2]https://www.zoomeye.org/project?id=industry
[3]https://censys.io/ipv4/help/definitions?q=&

vytvorení účtu pomocou Gmail adresy vytvorenej pre porovnanie užívateľ nedostane členstvo; tiež je pri dotazovaní možné zobraziť iba prvé dve strany, celkom 20 výsledkov. Účet vytvorený pomocou Gmail adresy je tiež možné previesť na účet s členstvom za jednorázový poplatok 49$. Pomocou vytvorených účtov s a bez členstva je možné používať aj všetky filtre okrem filtrov **vuln** a **tag**. Za deň je možné pokladať veľké množstvo dotazov, ktoré sa podarilo minúť po celom dni skúšania a hľadania optimálneho dotazu, čo je ale dostačujúce pre bežného používateľa. Pri vyhľadávaní bez účtu je však možné položiť iba 10 dotazov za deň. Obmedzenie na 10 dotazov za deň je priraďované k IP adrese, takže po pripojení do VPN siete bolo možné položiť ďalších 10 dotazov.

Okrem výhod pri vyhľadávaní s členstvom je tento účet ako jediný možné používať na Shodan Monitor, kde je možné sledovať 16 IP adries. Shodan Monitor je funkcia, pri ktorej si vieme nadstaviť sledované IP adresy a pri každej zmene nás Shodan o nej informuje na nastavenú e-mailovú adresu.

Pristupovať k API je možné pomocou API kľúča, ktorý dostane každý zaregistrovaný užívateľ. Pri účte bez členstva alebo predplatného je API dosť limitované, pretože nie je možné používať filtre, ale iba čisto text a príde iba prvých 100 výsledkov. Pre použitie filtrov a zobrazenie viacerých výsledkov sú potrebné dotazovacie kredity. Účet s členstvom má k dispozícii 100 kreditov. V prípade, že je výsledkov do 100, tak sa žiadny kredit nestrhne, ak je ich nad 100, strhne sa 1 kredit.

Pri účte s členstvom je k dispozícii aj 100 skenovacích kreditov. Dané kredity je možné použiť na aktuálne skenovanie IP adresy a zobrazenie zariadení, ktoré sa tam nachádzajú. Za každú skenovanú IP adresu je strhnutý 1 kredit.

Úplné informácie o účte s členstvom a predplatných sa nachádza na webovej stránke https://account.shodan.io/billing.

Shodan umožňuje aj prihlásenie pomocou účtu Google, Twitter alebo Windows Live. Po prihlásení pomocou účtu Google za použitia školskej adresy, kedy nebola vykonaná registrácia, účet na Shodane po pár dňoch prestal fungovať a nebolo možné sa prihlásiť. Pri používaní školskej e-mailovej adresy je preto potrebné sa najskôr zaregistrovať.

3.2.2 Účet Censys vyhľadávača

Censys tak isto ako Shodan umožňuje vyhľadávanie bez potrebnej registrácie, ale s tým rozdielom, že pri dotazovaní je možné používať aj filtre.

Pre vytvorenie účtu je potrebné vypísať meno a priezvisko, e-mailovú adresu, prihlasovacie meno, heslo, názov spoločnosti a telefónne číslo. Hlavnou nevýhodou pri registrácii je, že všetky údaje vrátane názvu spoločnosti a telefónneho čísla musia byť vyplnené, v opačnom prípade Censys nevytvorí účet. Pomocou telefónneho čísla

nie je vôbec potrebné overiť pravosť, a tak je možné použiť aj neexistujúce číslo; pri názve spoločnosti je možné napísať ľubovoľný znak. Po zaregistrovaní taktiež príde na e-mail potvrdzujúci odkaz, ktorým sa účet aktivuje. Pri vytváraní účtu pomocou školskej e-mailovej adresy, na ktorej je nadstavené automatické presmerovanie všetkých prichádzajúcich správ na súkromnú e-mailovú adresu e-mail s potvrdzovacím URL odkazom neprišiel. Toto sa nezmenilo ani po využití možnosti zabudnuté heslo a bolo potrebné napísať na podporu. Z podpory prišla odpoveď po 20 dňoch s tým, že potvrdenie účtu spravili manuálne a je možné sa prihlásiť. Počas vytvárania účtu pomocou Gmail adresy prebehla registrácia bez komplikácii. Rozdiel v počte dotazov za mesiac medzi účtom, ktorý bol vytvorený pomocou školskej adresy a Gmail adresy nie je žiadny. Nebol nájdený rozdiel medzi účtami vytvorenými za pomoci školskej adresy a Gmail adresy; na tomto vyhľadávači teda nie je žiadne zvýhodnené akademické členstvo.

S vytvoreným účtom je možné položiť 250 dotazov za jedno obdobie, ktoré sa ráta odo dňa založenia účtu. Pri založení účtu v pätnástom dni mesiaca je jedno obdobie počítané do pätnásteho dňa následujúceho mesiaca. Pre neregistrovaných užívateľov je obmedzený počet dotazov na 10 a toto obmedzenie je rovnaké ako pri Shodan vyhľadávači. Počet zobrazených výsledkov záleží od počtu dotazov; ak sa zadá dotaz na vyhľadanie, zobrazí sa stránka, kde sa nachádza 25 výsledkov a každá ďalšia stránka s výsledkami je počítaná ako nový dotaz. Neregistrovaní užívatelia majú k dispozícii 250 výsledkov za deň a registrovaní 6250 výsledkov za mesiac.

Pristupovať k dátam pomocou API vyžaduje autentifikáciu pomocou základného overenia HTTP. Pre overenie HTTP sa používa prihlasovacie meno, kde sa zadáva API ID a heslo, kde treba zadať API Secret. API ID a API Secret je možné nájsť v nastaveniach účtu. Používanie API sa viaže na 250 dotazov za jedno obdobie, preto je možné dotazovať vyhľadávač pomocou webového rozhrania a API, dokopy 250 krát za mesiac. Na rozdiel od vyhľadávania pomocou webového rozhrania sa pri API k jednému dotazu nevráti iba 25 výsledkov, ale 100.

3.2.3 Účet BinaryEdge vyhľadávača

BinaryEdge nedovoľuje vyhľadávať bez registrácie a aby bolo dovolené vyhľadávať je potrebné si založiť účet.

Pri zakladaní účtu je potrebné vypísať meno a priezvisko, názov spoločnosti, ktorý môže byť ako pri Censyse iba jeden znak, e-mail a heslo. Overenie pred prvým prihlásením prebieha ako u predchádzajúcich vyhľadávačoch pomocou e-mailu. Boli vytvorené taktiež dva účty na porovnanie. Jeden pomocou školskej adresy a druhý pomocou Gmail adresy, a v týchto účtoch sa nenachádza žiadny rozdiel, podmienky sú rovnaké, preto ani pri tomto vyhľadávači nie je zvýhodnené akademické členstvo

.

Počet dotazov a výsledkov je úplne rovnaký ako pri registrovaných užívateľoch na vyhľadávači Censys. Pri bezplatnej registrácií však nie je možné pristupovať k dátam zo senzorov a historickým dátam.

Pristupovať k dátam pomocou API je pri BinaryEdge rovnaké ako pri Censyse, avšak s jediným rozdielom, a to že pri dotazovaní sa vráti iba 20 výsledkov.

3.2.4 Účet ZoomEye vyhľadávača

Na ZoomEye vyhľadávači pre neregistrovaných užívateľov je možné pri dotazovaní používať filtre a pokladať neobmedzený počet dotazov.

Registrácia účtu na ZoomEye je rozdelená do troch krokov. V prvok kroku treba zadať e-mailovú adresu, opísať bezpečnostný kód a zadať kód, ktorý príde na e-mail. Mimo kódu je celá správa v čínskom jazyku. V druhom kroku treba zadať telefónne číslo, znova opísať bezpečnostný kód a zadať číselný kód z SMS správy, takže nie je možné použiť neexistujúce číslo ako pri Censyse. SMS správa už príde v anglickom jazyku a platnosť kódu je 5 minút. V poslednom kroku je potrebné iba zadať heslo a vytvoriť účet. Z dôvodu zadávanie telefónneho čísla bol vytvorený iba jeden účet, a to pomocou školskej e-mailovej adresy.

Počet výsledkov, ktorý je možný zobraziť pre neregistrovaných užívateľov je jedna strana, čo je 20 výsledkov a pre registrovaných je to 100 strán, čo je 2000 výsledkov. Počet dotazov, ktoré je možné položiť je neobmedzený pre všetkých.

Získavať dáta pomocou API pri ZoomEye vyhľadávači je možné dvoma spôsobmi, a to buď pomocou API kľúča, alebo prístupového tokenu. API kľúč je možné nájsť v nadstaveniach účtu a prístupový token je možné získať poslaním prihlasovacích údajov pomocou API, takže k dátam pomocou API môžu pristupovať iba registrovaný užívatelia. ZoomEye má na rozdiel od ostatných vyhľadávačov obmedzený počet výsledkov, ktoré môžeme získať pomocou API. Mesačne je tak možné stiahnuť pomocou API 20 000 výsledkov.

3.2.5 Výsledky vyhľadávania

Vyhľadávače sa porovnávali na základe výsledkov štyroch protokolov, pomocou ktorých je možné zistiť informácie o PLC zariadeniach. V tabuľke 3.1 sa nachádza počet prvotných výsledkov, ktoré boli vyhľadávané pomocou čísla portu daného protokolu. Tieto výsledky neobsahovali iba informácie o PLC zariadenia, a tak boli hľadané ďalšie filtre, aby boli zobrazované iba výsledky o PLC zariadeniach. Počet výsledkov, ktoré sú o PLC zariadeniach sa nachádzajú v tabuľke 3.2. Spôsob a použitie ďalších filtrov je samostatne rozobraté nižšie v podkapitolách.

Protokoly	Shodan	Censys	BinaryEdge	ZoomEye
Siemens S7	15 080	6 549	2 518 049	34 320
Modbus	6 053	29 118	3 203 631	26 669
Ethernet/IP	53 326	-	4 056 194	18 464
DNP3	467 494	519	3 866 517	12 524 658

Tab. 3.1: Počet prvotných výsledkov vyhľadávania.

Protokoly	Shodan	Censys	BinaryEdge	ZoomEye
Siemens S7	3 827	5 964	6 961	2 362
Modbus	152	1 567	2 497	1 862
Ethernet/IP	5 635	-	5 492	7 341

Tab. 3.2: Počet konečných výsledkov po použití viacerých filtrov.

Siemens S7

Zariadenia a služby, ktoré komunikujú pomocou tohto protokolu boli v prvom kroku pri Shodan, BinaryEdge a ZoomEye vyhľadávači dotazované pomocou filtru **port:102**, pri Censyse bolo potrebné použiť filter **ports:102**.

Po prvotnom vyhľadávaní bolo pri Shodane možné zistiť, že z celkového počtu výsledkov sa v 3057 prípadoch jednalo o komunikáciu pomocou OpenSSH nástroja, 858 zariadení boli Conpot honeypoty, v 58 prípadoch sa jednalo o SMTP démona, 58 zariadení komunikovalo pomocou Dropbear a nachádzalo sa tam 16 S61850 zariadení, ktoré slúžia ako ochrana proti elektrickému oblúku. Pre odstránenie týchto výsledkov bolo potrebné použiť ďalší filter **product:"Conpot, OpenSSH, Postfix smtpd, Dropbear sshd, S61850 for VAMP Relays"**, pred ktorým bol použitý znak „**-**“. Po dotazovaní pomocou dvoch spomenutých filtrov boli medzi výsledkami zariadenia, ktoré komunikovali pomocou HTTP protokolu a zariadenia, pri ktorých bol zachytený funkčný kód. Tieto výsledky boli ešte vyfiltrované pomocou príkazov **-HTTP**, **-00000000**, **-220** a **-RFB**. Konečný dotaz, ktorý bol použitý mal podobu **port:102 -product:"Conpot, OpenSSH, Postfix smtpd, Dropbear sshd, S61850 for VAMP Relays" -HTTP -00000000 -220 -RFB**, po ktorom bolo dostupných 3827 výsledkov, v ktorých sa nachádzalo malé percento zariadený iba s otvoreným portom 102. Tieto zariadenia sa inak pretriediť nedali, ale výsledky boli dostačujúce a pri väčšine zariadení bolo možné zistiť o aké zariadenie sa jedná.

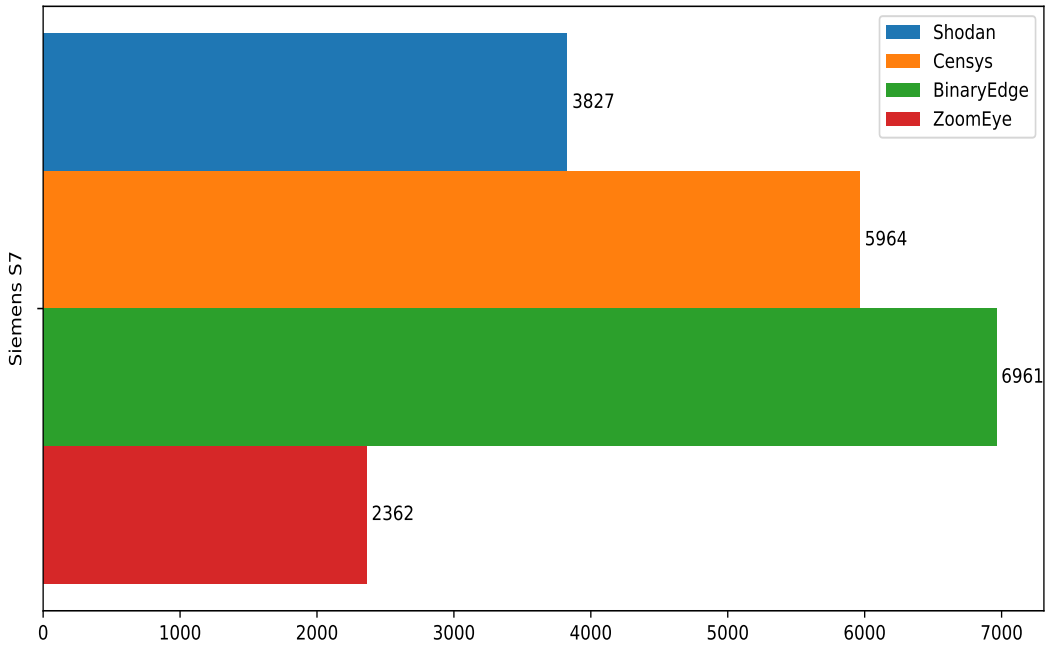
Pri Censyse je potrebné otvoriť výsledok aby bolo možné vidieť dáta nachádzajúce sa pri jednotlivých zariadeniach. Spolu s filtrom portu bol použitý filter pre protokol bežiaci na danom porte. Medzi prvým a druhým filtrom bolo použité slovo **AND** aby vyhľadávač vedel, že má zobraziť výsledky, pre ktoré platia oba filtre.

Celkový dotaz mal tvar **(ports:102) AND protocols: "102/s7"** a našlo sa 5964 výsledkov. Na prvej stránke bolo možné pri takmer všetkých výsledkoch zistiť ID zariadenia, vďaka ktorému je možné zistiť o aké PLC sa jedná. Niektoré výsledky neobsahovali žiadne údaje o zariadení a v niektorých prípadoch sa mohlo jednať o honeypot, pretože pri danom zariadení sa nachádzalo viac ako 30 bannerov. Dané výsledky sa nepodarilo odfiltrovať aby sa už naďalej nezobrazovali.

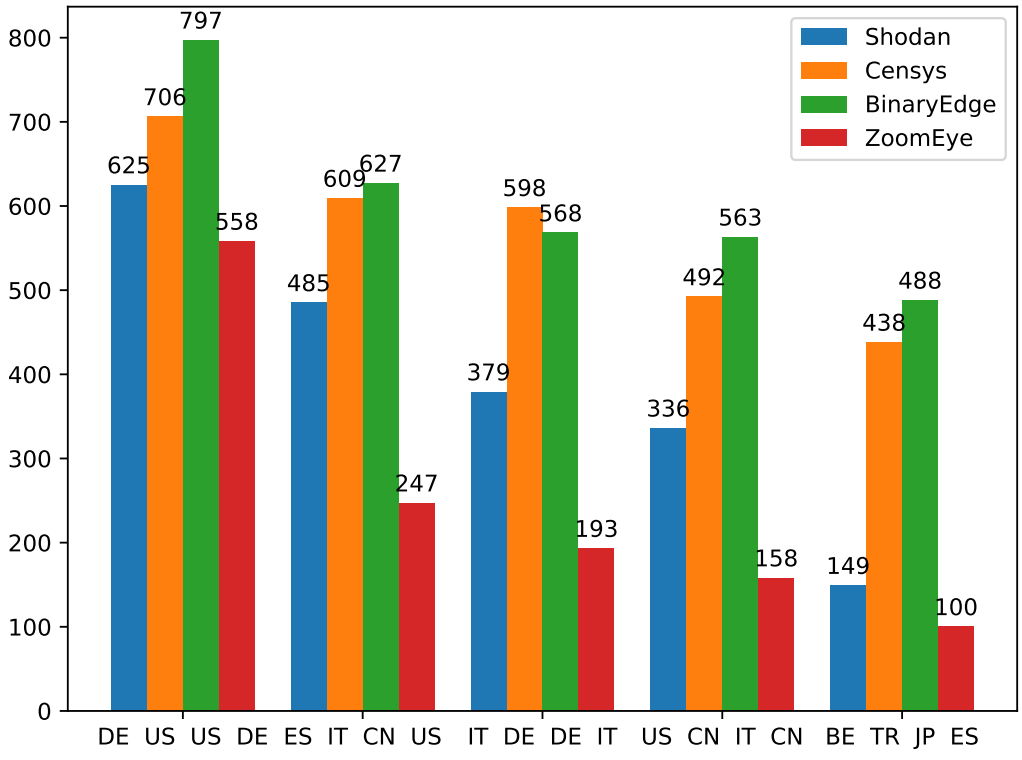
Pomocou vyhľadávača BinaryEdge sa pomocou filtru na port zobrazilo najviac výsledkov zo všetkých vyhľadávačov, čo je možné vidieť v tabuľke 3.1. Veľa výsledkov však bolo bez informácií o zariadení alebo bol zachytený HTTP banner, preto bol použitý ďalší filter pre produkt. Konečný dotaz mal tvar **port:102 product:"Siemens S7 PLC"**, vďaka ktorému sa zobrazovali výsledky s informáciami o PLC zriadení. Celkový počet výsledkov bol 6961. Niektoré výsledky neobsahovali žiadne informácie o PLC alebo obsahovali iba ID zariadenia ako pri Censyse, v niektorých prípadov sa dalo zistiť o aké PLC sa jedná a akú verziu operačného systému používa.

ZoomEye hneď po prvotnom dotazovaní zobrazoval zariadenia s popisom o aké zariadenie sa jedná. Vo výsledkoch sa vyskytovali aj záznamy z roku 2014 a neskôr. Vďaka tomu bolo možné zistiť, že najviac zariadení bolo nájdených v roku 2017, a to 19890. V prípade zobrazenia výsledkov z roku 2020 boli použité filtre **after:"2020-01-01"** a **before:"2021-01-01"**, pred ktorými bol použitý znak „**+**“. Výsledný filter **port:102 +after:"2020-01-01"+before:"2021-01-01"** stačil na to, aby nám vyhľadávač ukazoval zariadenia s bližšími informáciami, ktorých bolo ich 2326.

V grafe 3.1 je zobrazený počet vyhovujúcich výsledkov. Pri vyhľadávači Censys a BinaryEdge môžeme brať tento údaj iba ako informačný, pretože niektoré výsledky neobsahujú informácie o zariadení alebo je možné zistiť iba ID modulu. Vyhľadávače Shodan a ZoomEye dokážu zobrazovať výsledky, ktoré sú takmer presné našim požiadavkám a môžeme vedieť, že tieto čísla ukazujú počet vyhovujúcich výsledkov. Konečný počet výsledkov je v grafe 3.2 zobrazený ako počet zariadení v danej krajine.



Obr. 3.1: Počet výsledkov pre Siemens S7.



Obr. 3.2: Počet výsledkov na danú krajinu pre Siemens S7.

Modbus

Tak isto ako pri protokole Siemens S7 boli pri prvom dotazovaní použité filtre **port:502** a **ports:502**.

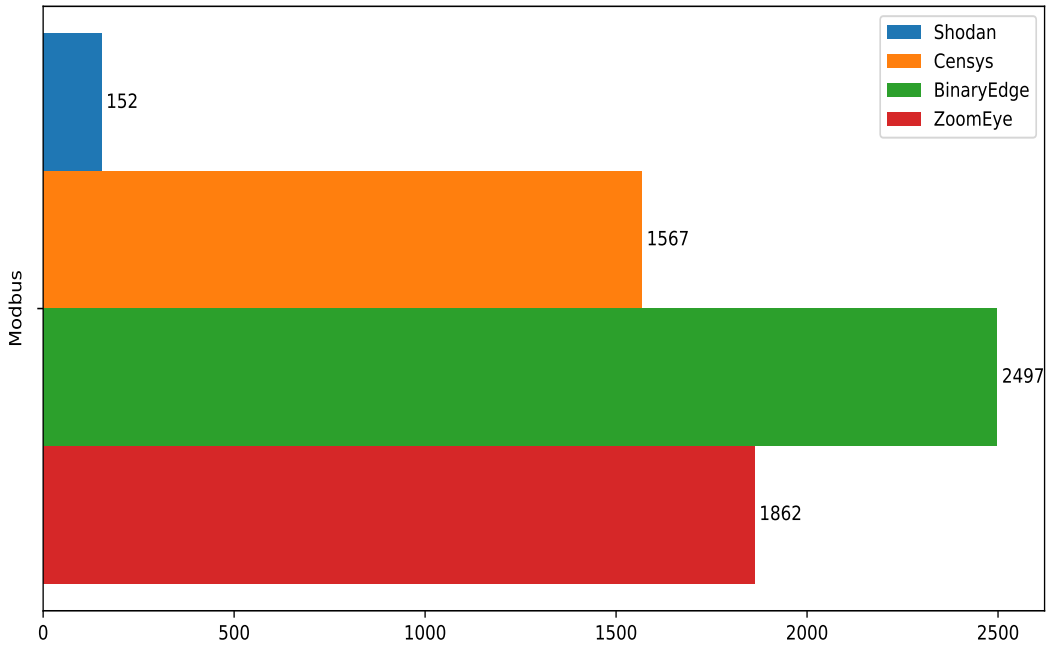
Shodan zobrazoval výsledky, pri ktorých neboli žiadne informácie o zariadeniach. Jednalo sa o výsledky kde bolo možné zistiť iba IP adresu a otvorené porty, nenachádzali sa tu však žiadne banery ani informácie o aké zariadenie sa jedná. Pri použití iných filtrov taktiež nebolo možné nájsť výsledky z informáciami o zariadení. Pre zobrazenie výsledkov s informáciami bola využitá možnosť kedy Shodan prehľadáva banery. Spolu s filtrom na port bol použitý v dotaze čisto iba text, a to **schneider OR siemens**, kde OR značí aby vyhľadávač zobrazil výsledky kde sa nachádza slovo schneider alebo siemens. Výsledný dotaz, ktorým bol Shodan dotazovaný bol **port:502 schneider OR siemens** a bolo zobrazených 152 výsledkov.

Z celkového počtu výsledkov, ktoré Censys vyhľadal sa v 1567 prípadoch jednalo o PLC zariadenie. Na zobrazenie čisto iba PLC zariadení bol použitý filter, ktorý pri protokole Siemens S7 nefungoval a to **tags.raw:"programmable logic controller"**. Výsledný filter, ktorý bol použitý pri Censys vyhľadávači bol **ports:502 AND tags.raw:"programmable logic controller"**.

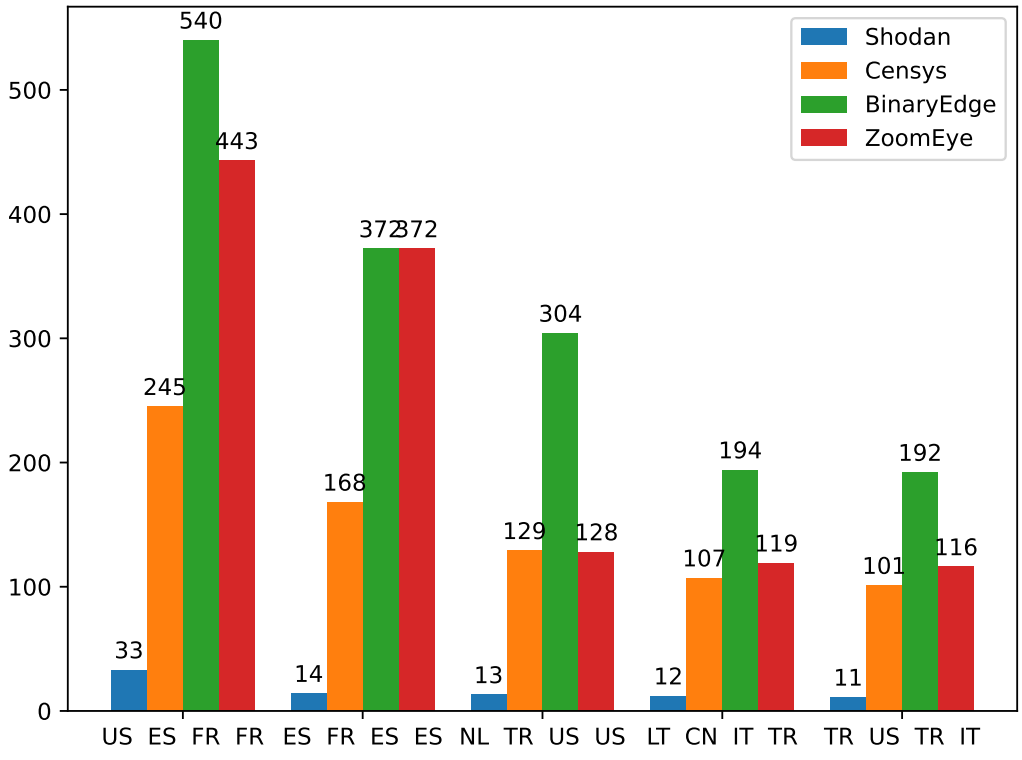
Tak isto ako pri vyhľadávači Shodan bolo pri BinaryEdge využité prehľadanie textu výsledku. Výsledný dotaz mal teda tvar **port:502 Schneider Electric** a bolo nájdených 2497 výsledkov. Vo výsledkoch sa nenachádzali iba PLC zariadenia, ale aj komunikačné brány alebo front–end procesory. Tieto zariadenia sa nedali inak odfiltrovať, pretože pri použití filtra **device:"PLC"** neboli nájdené žiadne výsledky. Konečný počet výsledkov nemožno brať ako počet nájdených PLC zariadení.

Pomocou ZoomEye vyhľadávača bolo nájdených 1862 PLC zariadení pri Modbus protokole. K tomuto počtu sa dopracovalo pomocou rovnakých filtrov ako pri Siemens S7 protokole pre rok 2020, ku ktorým sa pridal filter **device:"PLC"**, výsledný filter mal tak tvar **port:502 +after:"2020-01-01"+before:"2021-01-01"+device:"PLC"**.

Pre Modbus boli tiež vytvorené dva grafy. Graf 3.3 zobrazuje počet vyhovujúcich výsledkov pre vyhľadávač Shodan, Censys a ZoomEye. Počet výsledkov pri vyhľadávači BinaryEdge nemožno brať ako počet vyhovujúcich výsledkov, pretože sa tam nachádzajú aj iné zariadenia ako PLC. V grafe 3.4 sú tieto výsledky zoradené podla počtu zariadení v určitej krajine.



Obr. 3.3: Počet výsledkov pre Modbus.



Obr. 3.4: Počet výsledkov na danú krajinu pre Modbus.

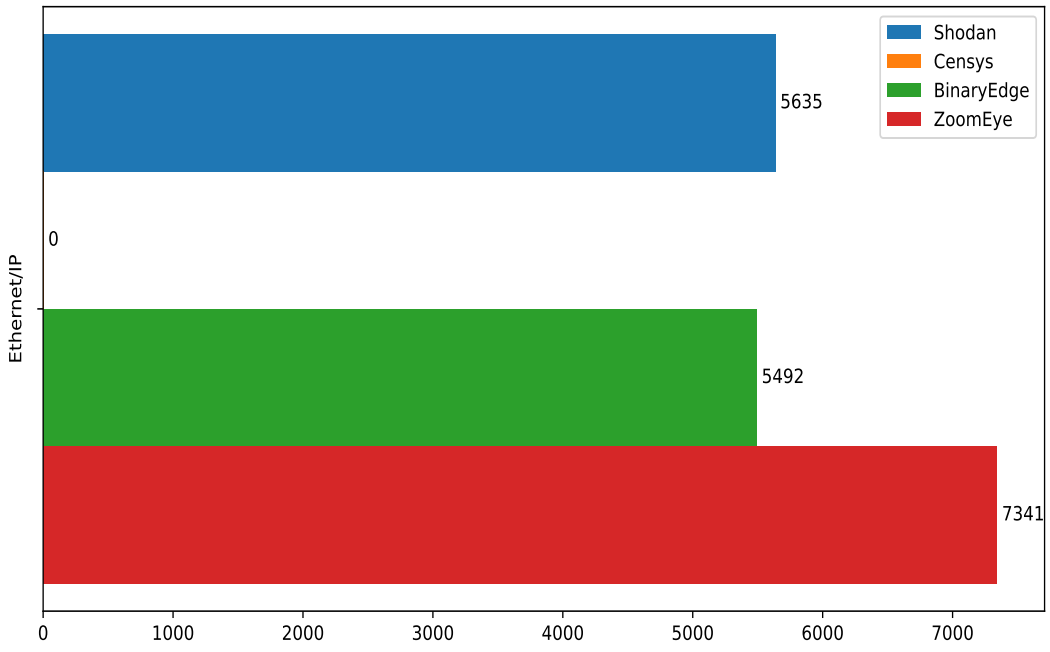
Ethernet/IP

Pri Ethernet/IP protokole bol použitý iba filter **port:44818**, pretože vyhľadávač Censys nedokáže vyhľadávať zariadenia pomocou tohoto portu.

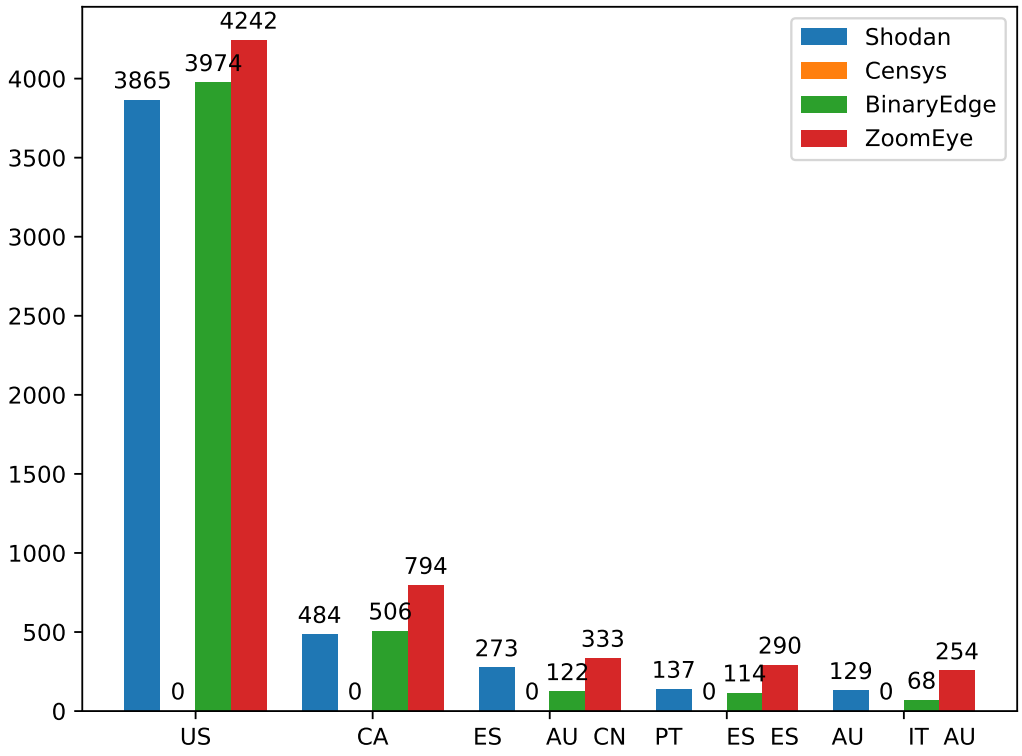
Pre dotazovanie Ethernet/IP protokolu pri Shodan a BinaryEdge vyhľadávači bolo okrem filtra na porty využité vyhľadávanie v banery. Pre vyhľadávanie v banery bol využitý text **Programmable Logic Controller**, po ktorom nebolo potrebné použiť iný filter, a tak výsledný dotaz bol **port:44818 Programmable Logic Controller**. Shodan po tomto dokázal zobrazovať 5635 výsledkov a BinaryEdge 5492 výsledkov, kde bolo možné zistiť o aké zariadenie sa jedná.

Pre vyhľadávanie zariadení pri ZoomEye vyhľadávači boli použité rovnaké filtre ako pri dotazovaní protokolu S7, kde bolo iba zmenené číslo portu a nájdených výsledkov bolo 7341.

Pre protokol Ethernet/IP boli vytvorené rovnaké grafy ako pri predchádzajúcich protokoloch. Výsledky, ktoré boli dosiahnuté pri Ethernet/IP protokole je možné si pozrieť v grafoch 3.5 a 3.6.



Obr. 3.5: Počet výsledkov pre Ethernet/IP.



Obr. 3.6: Počet výsledkov na danú krajinu pre Ethernet/IP.

DNP3

DNP3 protokol bol dotazovaný pomocou filtra **port:20000** a **ports:20000**.

Pomocou tohoto protokolu sa nepodarilo násť informácie o PLC zariadení ani pri jednom vyhľadávači.

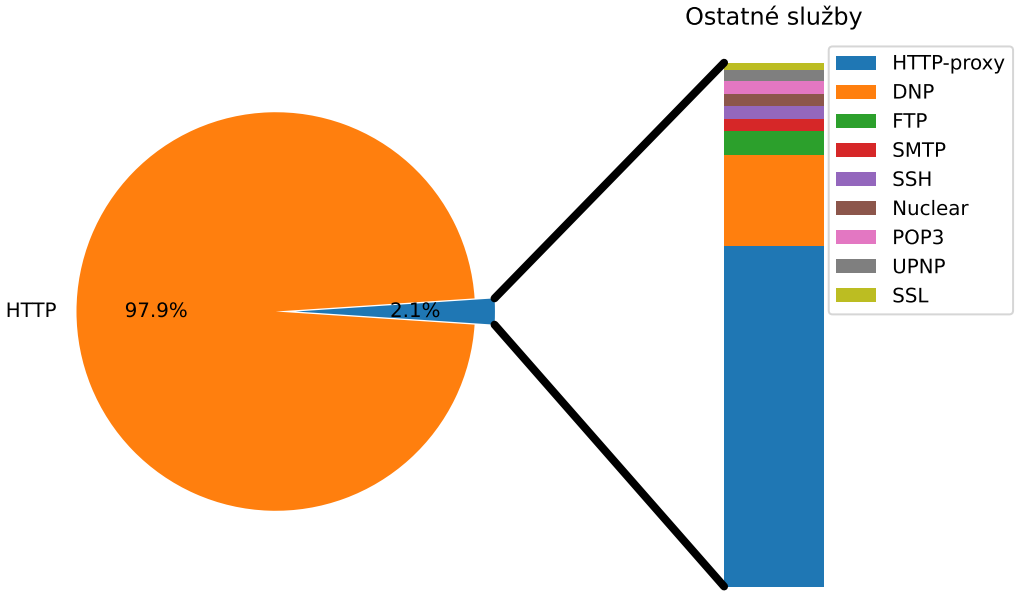
Shodan vo väčšine výsledkov zobrazoval HTTP baner s kódom 400. Nasledovali zariadenia, ktoré komunikovali pomocou SSH, pri ktorých boli informácie o SSH protokole. V zopár prípadoch bolo možné zistiť, že sa jedná o zariadenie F454, ktoré sa používa ako audio/video web server pre vzdialené ovládanie systému pomocou webových stránok alebo portálu MY HOME. Ďalej pri týchto zariadeniach bolo možné zistiť, že komunikuje pomocou protokolu OpenWebNet.

Pri Censys vyhľadávači sa pri veľkom počte výsledkov vyskytovala odpoveď v tvare **BWQFCwAAAQC68A==**. Občas sa podarilo nájsť zariadenie NPort 5210A, kedy sa jedná o komunikačnú bránu.

BinaryEdge spolu s filtrom **tag:ICS** dokázal vyhľadať iba 18 zariadení, kde v 8 prípadoch na porte 20000 bežal Modbus TCP protokol, v ďalších 8 prípadoch sa jednalo o framework Niagara, ktorý bol spomenutý pri protokole Ethernet/IP.

ZoomEye pri DNP3 protokole ponúkol najviac údajov o zariadeniach a dokázal vyhodnotiť a zoradiť najviac kategórií. Z celkového počtu záznamov 60 % vzniklo

v roku 2020 a z tohto počtu sa v 92 % prípadoch jednalo o zariadenia pripojené pomocou IPv6 adresy. V grafe 3.7 je možné vidieť, že v menej ako 98 % bol zachytený HTTP baner a viac ako 1 % výsledkov využívalo iné služby na porte 20 000.



Obr. 3.7: Služby na porte 20 000.

3.2.6 Vyhodnotenie porovnania

Pri porovnaní vyhľadávačov pomocou dokumentácie a informácii z webovej stránky by na vyhľadávanie PLC zariadení a skenovanie ICS sietí bol najlepší Shodan alebo ZoomEye. Censys vyhľadávač ma nevýhodu, že je schopný vyhľadávať iba pomocou 4 ICS portov a BinaryEdge nemá dostupných veľa informácii.

V prípade vyhľadávania bez registrácie je najlepšie používať ZoomEye, prípadne Shodan. Pri ZoomEye vyhľadávači je možné pokladať neobmedzený počet dotazov s tým, že je možné zobraziť iba prvých 20 výsledkov. Shodan umožňuje zobraziť rovnaký počet výsledkov, ale počet dotazov je obmedzený na 10 za deň.

Pri registrácii na ZommEye a Censys je potrebné zadávať telefónne číslo. Pri Censyse je možné zadať neexistujúce číslo, ale pri ZoomEye je potrebné SMS overenie.

Pre porovnanie výsledkov vyhľadávačov je možné z grafov a tabuľky 3.2 vidieť, že každý vyhľadávač sa pri každom protokole správa inak. Pomocou BinaryEdge sa podarilo nájsť najviac informácií o PLC zariadeniach.

V prípade hľadania pomocou filtru **tag:ICS** bolo nájdených málo zariadení, preto nie je vhodné skenovanie ICS sieti pomocou tohoto filtru, ale je potrebné používať viaceré iné filtre.

Pri Censyse je nevýhoda, že pre zobrazenie informácii je potrebné otvoriť jednotlivé výsledky, ale v prípade použitia správnych filtrov vie zobrazovať pomerne presné výsledky. Shodan dokáže taktiež zobrazovať presné výsledky a dokáže zobrazovať počty zariadení, pri ktorých sa nachádzajú informácie o zariadení. Najlepšie sa pracovalo so ZoomEye, tento vyhľadávač dokáže ako jediný zobrazovať odporúčané dotazy, má najviac štatistík výsledkov, ako napríklad rok vzniku záznamu, služby bežiace na danom porte, o aké zariadenia sa jedná, firmy, ktorým dané zariadenie patrí a mnoho ďalších.

Z dosiahnutých výsledkov porovnania sa prišlo k záveru, že vyhľadávač BinaryEdge je schopný vyhľadať najviac výsledkov. Najväčšia nevýhoda tohoto vyhľadávača je, že pri bezplatnom účte je možné pomocou API pristupovať iba k 5000 výsledkom za mesiac, preto nebude využitý pri tvorbe aplikácie. Censys vyhľadal pomerne presné výsledky za použitia viacerých filtrov. Tento vyhľadávač však dokáže vyhľadávať malé množstvo ICS protokolov, preto tiež nebude použitý pri tvorbe aplikácie. Shodan a ZoomEye mali zaujímavé výsledky a každý dokázal zobraziť potrebné údaje pre každý protokol. Tieto vyhľadávače budú porovnané aj na základe API, podľa čoho bude rozhodnuté, ktorý vyhľadávač bude použitý pri tvorbe aplikácie.

4 Práca s API

Hlavným cieľom tejto kapitoly je práca s API jednotlivých vyhľadávačov. Práca s API bola vyskúšaná pomocou aplikácie postman, na základe čoho bol vybraný vyhľadávač, ktorý sa použije pri tvorbe aplikácie. V podkapitole 4.1 je popísané API a ich základné rozdelenie. V podkapitole 4.2 sú popísané a zobrazené jednotlivé výsledky vyhľadávania pomocou API pre vyhľadávače, ktoré boli vybraté ako najvhodnejšie v podkapitole 3.2.6.

Postman

Postman je vývojový nástroj API, ktorý vývojárom uľahčuje vytváranie, zdieľanie, testovanie a dokumentovanie API a je dostupný pre operačné systémi Windows, OS X a Linux. Slúži k návrhu a interakciu s HTTP API, pričom umožňuje aj písanie automatických testov, mock server, monitorovanie, tvorbu dokumentácie a jej zdieľanie v tíme. Má schopnosť vytvárať rôzne typy HTTP požiadaviek (GET, POST, PUT, PATCH, atď.), ukladať prostredia pre neskoršie použitie a prevádzať API na kód v rôznych jazykoch. Postman taktiež umožňuje spoluprácu v reálnom čase, kedy sa všetci členovia tímu môžu pripojiť v jeden moment a zároveň vykonávať zmeny alebo tvoriť novú kolekciu API [63].

4.1 API

Application programming interface (API) je rozhranie využívané pri vývoji mobilných a webových aplikácií a tvorbe internetových stránok. Hlavným cieľom API je komunikácia medzi dvomi platformami, ktoré si navzájom vymieňajú dáta.

Existuje mnoho rôznych typov API a spôsobov jeho kategorizácie. Z hľadiska prístupu k API je ho možne rozdeliť na:

- Interné API – súkromné API, ktoré je používané v rámci jednej organizácie.
- Externé API – verejné API, ktoré je k dispozícii komukoľvek.
- Partnerské API – súkromné API, ktoré používajú len partnerské organizácie.

Pokiaľ sa jedná o architektúru API, existuje niekoľko štýlov. Najpopulárnejšie štýly sú [64]:

- REST API – Rozhrania REST (REpresentational State Transfer) API sú najbežnejšie rozhrania API, ktoré sa používajú pri webových stránkach. Boli navrhnuté tak, aby využívali existujúce protokoly a pri webových stránkach najčastejšie využíva protokol HTTP.

- Webhooks – jedná sa o automatizované správy odosielané z jedného systému do druhého vždy, keď dôjde k nejakej udalosti. Webhooks sa označujú aj ako reverzné API a používajú sa na kontrolu zmien údajov.
- SOAP API – SOAP (Simple Object Access Protocol) API sú štrukturovanejšie a formálnejšie ako iné rozhrania API, sú spoľahlivé a dôveryhodné, ale môžu byť pomalšie ako ostatné API. Používa protokol správ založený na XML, ktorý podľa potreby koncového bodu obsahuje značky obálok, hlavičiek a tela.
- GraphQL API – GraphQL (Graph Query Language) pôvodne vytvoril Facebook ako interný nástroj v roku 2012, v roku 2015 ho verejne vydali ako open-source jazyk pre API. GraphQL definuje ako jedno API, ktoré žiada iné API o informácie; namiesto toho, aby sa spoliehal na to, ako server definuje koncový bod môže dotaz GraphQL požiadať iba o konkrétnu informáciu.
- WebSocket API – spoliehajú sa na komunikačný protokol WebSocket, ktorý je plne duplexný komunikačným kanálom cez jediné pripojenie TCP. Rozhrania WebSocket API poskytujú serverom štandardný spôsob odosielania informácií a údajov klientom aj v prípade, že klient údaje nežiada.

4.2 API jednotlivých vyhľadávačov

V tejto podkapitole je popísaná práca s API Shodan a ZoomEye vyhľadávača. Prvotné dotazovanie API bolo vykonané pomocou aplikácie Postman, aby sa zistilo ako sú dáta štrukturované.

4.2.1 API Shodan vyhľadávača

Pre prácu s API Shodan vyhľadávača, bola do Postman aplikácie stiahnutá kolekcia Postman Shodan Collection z GitHubu[1]. Pomocou tejto kolekcie bol Shodan dotazovaný a pri dotazovaní vyhľadávača na základe portu 102 prišlo prvých 100 výsledkov. Okrem výsledkov prišiel aj údaj koľko je celkovo výsledkov na daný dotaz. Celkový počet výsledkov na daný dotaz bol rovnaký ako pri prvotnom vyhľadávaní pomocou webového užívateľského rozhrania.

Celková API odpoveď bola veľmi dlhá a preto nižšie budú rozobraté iba jednotlivé časti. Najdôležitejšia časť API odpovede je sekcia `data` a `ip_str`, ktoré sú zobrazené vo výpise 4.1. V sekcii `data` sa nachádzajú informácie o danom zariadení a v `ip_str` sa nachádza IP adresa zariadenia.

Ďalšie zaujímavé informácie sa týkajú polohy, komu zariadenie patrí a kedy bolo nájdené. Tieto informácie sa nachádzajú v sekciách `location`, `org` a `timestamp`, ako je možné vidieť vo výpise 4.2.

[1] https://github.com/bitnesswise/shodan-postman-collection

Výpis 4.1: Sekcia data a ip_str z API odpovede.

```
"data": "Basic␣Hardware:␣6ES7␣214-1AG40-0XB0␣␣v.0.5\n
Module:␣6ES7␣214-1AG40-0XB0␣v.0.5\n
Basic␣Firmware:␣6ES7␣214-1AG40-0XB0␣v.4.4.1\n",
"ip_str": "37.81.174.185"
```

Výpis 4.2: Sekcia location, org a timestamp z API odpovede.

```
"location": {
    "city": "Horn-Bad␣Meinberg",
    "region_code": "NW",
    "country_code": "DE",
    "country_name": "Germany" },
"org": "Deutsche␣Telekom␣AG",
"timestamp": "2020-12-11T08:29:00.304425",
```

Okrem základných informácii je možné z API dozvedieť sa to, ktorý vyhľadávač toto zariadenie našiel, cez akého poskytovateľa internetového pripojenia je zariadenie prístupné a aké tagy zariadenie dostalo.

4.2.2 API ZoomEye vyhľadávača

Pri práci s API ZoomEye vyhľadávača bolo potrebné v Postmane vytvoriť dotazy, pretože žiadna kolekcia nebola nájdená. Pristupovať k dátam pomocou API pri ZoomEye vyhľadávači ide pomocou API kľúča alebo pomocou prístupového tokenu. Pri Shodan vyhľadávači sa pristupovalo k dátam pomocou API kľúča, preto pri ZoomEye bolo vyskúšané pristupovať k dátam pomocou prístupového tokenu. Prístupový token je možné získať pomocou API po odoslaní POST požiadavky, v ktorej tele sa nachádzajú prihlasovacie údaje, ako je možné vidieť vo výpise 4.3. Výpis 4.4 zobrazuje odpoveď na požiadavku o prístupový token. Prístupový token pre ZoomEye vyhľadávač je dlhý 192 znakov; z toho dôvodu a tiež aj kvôli tomu, že sa jedná o súkromný údaj je vo výpise len jeho začiatok. Prístupový token je následne odosielaný v autorizačnej hlavičke GET požiadavky, aby bolo možné pristupovať k výsledkom vyhľadávača.

Výpis 4.3: JSON štruktúra prihlasovacích údajov.

```
{    "username": "xdanko06@vutbr.cz",
     "password": "*****************" }
```

Výpis 4.4: Odpoveď z požiadavky o prístupový token.

```
{    "access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6Ik..."}
```

Po získaní prístupového tokenu bola vytvorená GET požiadavka, vďaka ktorej bolo možné pristupovať už k samostatným dátam vyhľadávača.

Pomocou vytvorenej GET požiadavky bol vyhľadávač dotazovaný s filtrom **port:102**. V odpovedi prišlo prvých 20 výsledkov spolu s údajom koľko existuje výsledkov pre daný dotaz. Pomocou API je možné pristúpiť k 31 750 výsledkom, pričom pomocou webového rozhrania je možné pristúpiť k 34 320 výsledkom. Pomocou filtra **port:102 +after:"2020-01-01"+before:"2021-01-01"** bolo pomocou API nájdených 2 211 výsledkov, pričom pri webovom rozhraní 2 326. Pri použití viacerých filtrov je rozdiel v počte výsledkov medzi API a webovým rozhraním minimálny.

Štruktúra API odpovede pri ZoomEye vyhľadávači sa od Shodan odpovede veľmi nelíši. Rozdiely odpovedí boli iba v pomenovaniach sekcií. Napríklad sekcia s IP adresou je pri ZoomEye pomenovaná ako **ip** a informácie o PLC zariadení sa nachádzali v sekcii **banner**, ako je možné vidieť vo výpise 4.5.

Výpis 4.5: Sekcia ip a banner z API odpovede.

```
"ip": "178.145.167.1",
"banner": "\n␣␣Module:␣6ES7␣214-1HG40-0XB0␣\n
Basic␣Hardware:␣6ES7␣214-1HG40-0XB0␣\n␣␣Version:␣4.1.3"
```

4.2.3 Vyhodnotenie práce s API

Štruktúra jednotlivých API odpovedí sa veľmi nelíši a dotazovanie vyhľadávačov bolo bezproblémové. Pri tvorbe aplikácie bude ale použité API Shodan vyhľadávača z viacerých dôvodov. Prvý dôvod, prečo bolo vybrané API Shodan vyhľadávača je, že na Shodane je možné mať so školským e-mailom akademické členstvo, ktoré má k dispozícii 100 dotazovacích kreditov. Pomocou 100 dotazovacích kreditov je teda možné pristúpiť k minimálne 10000 výsledkom za mesiac. Minimálne 10000 výsledkov je z toho dôvodu, že 1 kredit je stiahnutý za dotaz, pre ktorý je k dispozícii viac ako 100 výsledkov. Preto pri dotaze, pre ktorý existuje 4700 výsledkov sa stiahne iba 1 kredit a je jedno či sa stiahnu všetky výsledky alebo len prvých 100. Ďalšie dôvody sú, že ZoomEye vyhľadávač má niektoré dokumentácie a fóra iba v čínskom jazyku a pri tvorbe účtu je potrebné zadávať telefónne číslo, aby sme získali API kľúč.

5 Praktická implementácia vyhľadávacieho nástroja

Podľa zadania bakalárskej práce bola vytvorená aplikácia na ukladanie výsledkov z vyhľadávača Shodan do databáze. Výsledky, ktoré sa ukladajú sú o PLC zariadeniach, konkrétne dátum a čas vyhľadania PLC Shodanom, IP adresa, informácie o PLC zariadení, krajina a mesto kde sa zariadenie nachádza. V prípade, ak sa pri zariadení nachádzajú aj zraniteľnosti, na ktoré je dané zariadenie zraniteľné, ukladajú sa aj označenia zraniteľnosti. V tejto kapitole bude popísaný vývoj nástroja od vytvorenia SQL databázy až po grafické užívateľské prostredie a bude popísaná funkcionalita a využitie jednotlivých častí užívateľského rozhrania.

5.1 Vývoj nástroja

Vývoj nástroja prebiehal v prostredí Visual Studio 2019 v jazyku C# s využitím NuGetu Shodan, kedy sa jedná o knižnicu asynchrónneho C# klienta pre shodan.io Rest API, napísanú v jazyku Go. Grafické užívateľské rozhranie bolo vytvorené vo WPF, čo je knižnica tried pre tvorbu grafického rozhrania od spoločnosti Microsoft. Navrhnutý nástroj dokáže zozbierať informácie o Siemens, Allen-Bradley a Schneider Electric PLC zariadeniach zo Shodan vyhľadávača pomocou REST API a uložiť ich do databázy. Uložené dáta je možné následne filtrovať, vyhľadávať v nich požadované parametre a zobraziť ich vo vytvorenom nástroji.

Nástroj používa SQL databázu Microsoft SQL Server 2019 Developer Edition; jedná o bezplatnú edíciu s kompletnou sadou funkcií, ktorá je licencovaná k použitiu pre vývoj a testovanie v neprodukčnom prostredí. Na konfiguráciu SQL servera, vytvorenie databázy a tabuľky bol použitý program Microsoft SQL Server Management Studio 18. Prístup do databázy bol zabezpečený pomocou SQL Server autentifikácie, kde je potrebné zadať prihlasovacie meno a heslo. Tabuľka, ktorú nástroj používa bola vytvorená pomocou skriptu, ktorý je možné vidieť vo výpise 5.1.

Vytvorená tabuľka obsahuje niekoľko stĺpcov s údajmi, konkrétne sa jedná o:

- `ID` – hodnota typu `int`, ktorá slúži ako primárny kľúč daného výsledku. Hodnota sa dopĺňa automaticky od 1 a každým výsledkom sa zvyšuje o 1.
- `Date` – údaj typu `datetime` slúži na uloženie dátumu a času, kedy bolo dané zariadenie vyhľadané Shodan vyhľadávačom.
- `IP` – stĺpec IP sa používa na ukladanie IP adries daných výsledkov; hodnota IP stĺpca je typu `nvarchar` s maximálnym počtom znakov 16.
- `PLCinfo` – údaje v tomto stĺpci sú typu `nvarchar` s maximálnym počtom znakov 2000 a ukladajú sa sem informácie o PLC, ktoré boli zachytené z banera.

Výpis 5.1: Skript pre vytvorene SQL tabuľky.

```
CREATE TABLE [dbo].[APIresults] (
    [ID]       INT              IDENTITY (1, 1) NOT NULL,
    [Date]     DATETIME         NOT NULL,
    [IP]       NVARCHAR (16)    NULL,
    [PLCinfo]  NVARCHAR (2000)  NULL,
    [Country]  NVARCHAR (255)   NULL,
    [City]     NVARCHAR (255)   NULL,
    [Vulns]    NVARCHAR (1000)  NULL,
    [BrandID]  INT              NULL,
    CONSTRAINT [PK_APIresults]
    PRIMARY KEY CLUSTERED ([ID] ASC)
);
```

- `Country`, `City` – na ukladanie štátu a mesta, kde sa PLC nachádza slúžia tieto stĺpce, ktorých hodnoty sú typu `nvarchar` s maximálnym počtom znakov 255.
- `Vulns` – v poslednom stĺpci, do ktorého sa ukladajú dáta z API je hodnota údajov `nvarchar` s maximálnym počtom znakov 1000. Ukladajú sa sem zraniteľnosti, na ktoré je dané PLC zraniteľné.
- `BrandID` – je pomocná hodnota typu `int`, ktorá označuje výrobcu daného zariadenia a používa sa aj pri filtrovaní výsledkov na základe výrobcu. Hodnota int bola použitá z dôvodu rýchlejšieho prehľadávania tabuľky ako v prípade, keby by sa mal vyhľadávať celý názov výrobcu.

Po vytvorení a nadstavení databázy a tabuľky bol vytvorený samostatný nástroj na ukladanie a zobrazovanie výsledkov zo Shodan vyhľadávača. Základom nástroja sú triedy `ShodanAPI` a `DataAccessLayer`.

Trieda `ShodanAPI` obsahuje metódy, ktoré využívajú Nugget Shodan. Slúži na vytváranie a odosielanie dotazov a prijíma REST API odpovede. Okrem metód na vytváranie dotazov sa tu nachádzajú metódy na overenie API kľúča a zistenie zostávajúcich kreditov. Po prijatí odpovede sa dáta predajú triede `DataParser`, ktorá ich roztriedi a pripraví dáta do požadovaného formátu pred uložením.

`DataAccessLayer` trieda ukladá roztriedené dáta a zobrazuje, vyhľadáva a maže uložené dáta z databázy. Pripojenie k databáze sa vytvára v konštruktore tejto triedy, kedy je potrebné použiť pripojovací reťazec. Všetky spomenuté akcie sa vykonávajú pomocou LINQ. Aby bolo možné dotazovať databázu pomocou LINQ bola vytvorená LINQ to SQL trieda `DbRepo`. Po otvorení triedy `DbRepo` sa zobrazí objektovo relačný dizajnér, do ktorého sa vloží tabuľka z databázy a program si sám vygeneruje kód, ktorý slúži ako mapovanie medzi schémou databázy a objektmi.

Posledná trieda je `ExportData`, ktorá sa stará o export zobrazených dát do Excel súboru.

5.2 Grafické užívateľské prostredie

Ako bolo už skôr spomenuté, grafické užívateľské rozhranie bolo vytvorené vo WPF. Po spustení aplikácie sa zobrazí pomocné okno, ktoré je zobrazené na obrázku 5.1.

Obr. 5.1: Okno k uloženiu API kľúča.

Do políčka `API key` sa vkladá API kľúč zo Shodan vyhľadávača. Tlačidlo `Show data` slúži na zobrazenie hlavného okna, v ktorom je možné zobrazovať dáta z databázy v prípade, že nebude použitý API kľúč. Po kliknutí na tlačidlo `Save and Continue` si nástroj API kľúč uloží, aby bolo možné sťahovať nové výsledky pomocou API. Po uložení kľúča sa otvorí hlavné okno, ktoré je možné vidieť na obrázku 5.2.

Obr. 5.2: Hlavné okno vyhľadávacieho nástroja.

Sekcia `Query parameters`, ktorá sa nachádza v pravej hornej časti hlavného okna, slúži na nastavenie parametrov API dotazu. V tejto časti je možné vybrať výrobcu PLC zariadení, ktoré chceme vyhľadávať a uložiť do databázy, alebo zadať IP adresu, na ktorej sa majú vyhľadať PLC zariadenia. Vždy je možné zvoliť iba jeden

parameter; ak sa zvolí parameter IP, tak na zadanej IP adrese sa skúsia vyhľadať PLC zariadenia všetkých výrobcov, ktorých je možné zvoliť v parametroch. Okrem parametrov sa tu nachádza aj informácia o tom, koľko dotazovacích kreditov ešte ostáva. Po zvolení parametru a stlačení tlačidla `Save results` aplikácia začne sťahovať výsledky pomocou API a ukladať ich do databázy. Ak sa v pomocnom okne, ktoré sa zobrazí po spustení aplikácie stlačilo na tlačidlo `Show data`, táto sekcia je neprístupná a nie je možné ju používať.

V `Show/Delete parameters` sekcii sa vyberá parameter na zobrazenie alebo vymazanie zvolených výsledkov z databázy. Nachádzajú sa tu tlačidlá `Show results` a `Delete results`. Po kliknutí na jedno z tlačidiel sa výsledky zvoleného parametra zobrazia v šedej časti hlavného okna alebo vymažú z databázy.

Posledná sekcia, ktorá sa nachádza na pravej strane hlavného okna slúži k vyhľadávaniu zadaného výrazu vo výsledkoch. Vyhľadávaný výraz sa vkladá do políčka nad tlačidlom `Search` a daný výraz sa vyhľadáva v stĺpcoch tabuľky, kde sa ukladajú údaje z banera, mesto, štát a zraniteľnosti. Ak sa vyhľadávaný výraz nachádza v niektorých výsledkoch, tak sa dané výsledky zobrazia v šedej časti.

Okrem spomínaných sekcií sa dole na pravej strane hlavného okna nachádzajú tlačidlá `Change API key` a `Exit`. `Change API key` slúži na zobrazenie pomocného okna aby bolo možné pridať alebo zmeniť API kľúč a tlačidlom `Exit` sa aplikácia vypína.

Ako už bolo spomínané, šedá časť hlavného okna slúži na zobrazovanie výsledkov z databázy. Pod touto časťou je možné vidieť tlačidlá `Delete selected result`, ktoré slúži na odstránenie označeného výsledku z databázy, a `Export to Excel`, vďaka ktorému sa zobrazené výsledky v šedej časti uložia do Excel súboru. Po stlačení `Export to Excel` vyskočí dodatočné okno, v ktorom sa zvolí názov a cieľ uloženia súboru.

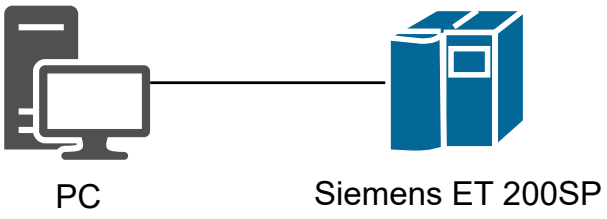
6 Práca s PLC zariadením

Po vytvorení aplikácie bolo zapojené PLC zariadenie spoločnosti Siemens. Jednalo sa presne o zariadenie ET 200SP, ktorého CPU má rovnaké funkcionality ako CPU 1511 alebo 1513 rodiny radičov S7–1500. PLC bolo zapojené do verejnej siete, aby sa zistilo, za aký čas a aké informácie o ňom vyhľadávače dokážu nájsť.

V tejto kapitole bude popísaná konfigurácia PLC, následné zapojenie a overenie zapojenia radiča do verejnej siete. Po zapojení do verejnej siete boli sledované vyhľadávače, aby sa zistilo, za ako dlho po zapojení sa PLC objaví vo výsledkoch. Po objavení informácii o PLC budú tieto informácie stiahnuté zo Shodan vyhľadávača do databázy pomocou vytvorenej aplikácie.

6.1 Konfigurácia PLC zariadenia

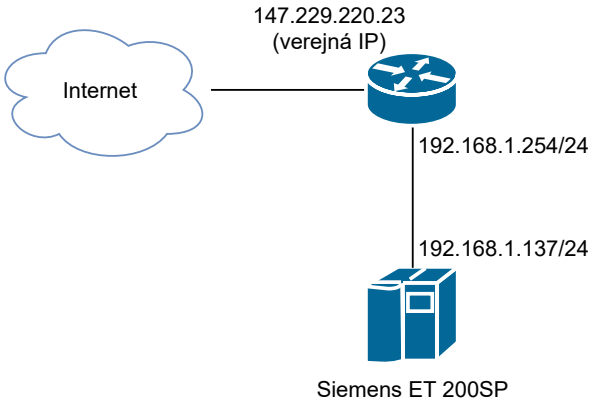
PLC zariadenie bolo pri konfigurácii pripojené priamo do ethernetového portu na PC, ako je možné vidieť na obrázku 6.1. Pre konfiguráciu PLC bol použitý program TIA Portal V16, ktorý je možné stiahnuť na Siemens stránke po zaregistrovaní účtu. Tia Portal sa stiahne spolu s trial verziou, vďaka ktorej je možné pridávať zariadenia do projektu 21 dní od jej aktivácie. Po vypršaní trial licencie je možné ďalej konfigurovať a pripájať sa k zariadeniam, ktoré sú pridané v projektoch, ale nie je možné pridávať zariadenia do existujúcich alebo nových projektov. PLC bolo zapojené, aby sa zistilo, za ako dlho ho dokážu vyhľadávače vyhľadať a aké informácie dokážu nájsť. Na routeri, cez ktorý pristupuje PLC do verejnej siete je LAN sieť s IP adresou 198.168.100.0/24. Preto bola v PLC nakonfigurovaná IP adresa routeru, konkrétne 192.168.1.254 a IP adresa radiča, ktorému bola pridelená IP adresa 192.168.1.137. Ďalej bolo nadstavené heslo k plnému prístupu k PLC, ako je zapisovanie a čítanie údajov zo vzdialeného bodu pomocou programu TIA Portal V16.



Obr. 6.1: Zapojenie PLC počas konfigurácie.

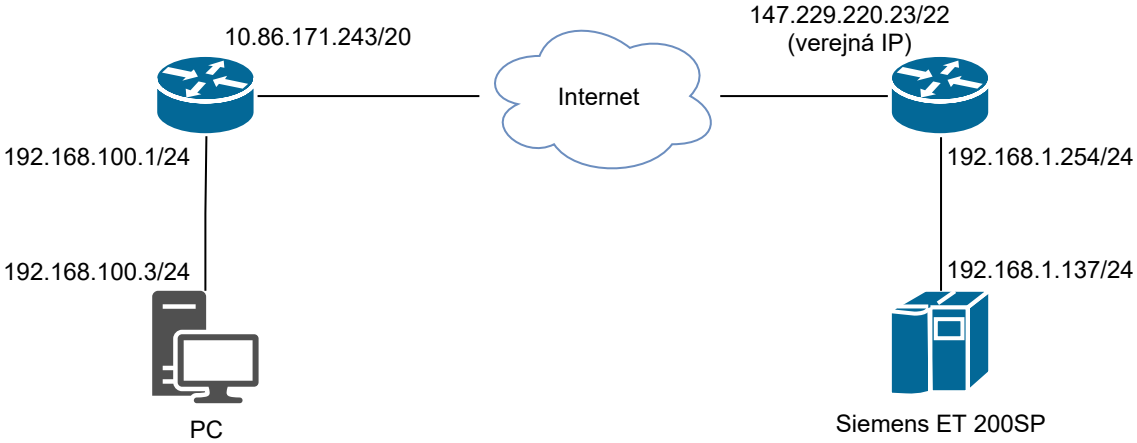
6.2 Zapojenie a overenie dostupnosti PLC zariadenia

Po nakonfigurovaní bolo PLC zapojené do verejnej siete cez router, ako je možné vidieť na obrázku 6.2. Po zapojení sa overilo nastavenie PLC z LAN siete, kedy bolo PLC pomocou TIA Portalu vyhľadané v LAN sieti a pripojenie prebehlo tiež bez problémov.



Obr. 6.2: Zapojenie PLC do verejnej siete.

Po bezproblémovom vyhľadaní a pripojení z LAN siete bolo vyskúšané pripojenie na PLC z verejnej siete. Vyhľadanie PLC je možné iba ak sa PC s Tia Portálom nachádza v rovnakej LAN sieti ako PLC. Pri prvom pokuse pripojenia na PLC sa nepodarilo pripojiť. Pre možnosť pripojenia sa na PLC z verejnej siete bolo potrebné nadstaviť na routeri presmerovanie portu. PLC zariadenia spoločnosti Siemens komunikujú cez port 102, preto všetka prichádzajúca komunikácia na tento port bola presmerovaná na IP adresu 192.168.1.137, ktorá patrí PLC zariadeniu.



Obr. 6.3: Overenie zapojenia PLC do verejnej siete.

PLC zariadenie bolo pripojené do verejnej siete v Česku. Obrázok 6.3 znázorňuje cestu úspešného pripojenia k PLC zo Slovenska. Po pripojení z verejnej siete je možné sledovať stav PLC, presnejšie čas doby cyklu, stav pamätí a režim CPU. Okrem sledovania je možné spustiť alebo zastaviť prevádzkový režim CPU a zresetovať prevádzkovú pamäť. Po pripojení je možné zistiť aj všetky informácie o PLC, ako je operačný systém, históriu režimu CPU a mnoho ďalších.

Pre nahratie nového nastavenia PLC alebo prevádzkového programu je potrebné byť odpojený od PLC. Po nakonfigurovaní nastavení alebo po vytvorení prevádzkového programu je potrebné najskôr projekt skompilovať. Skompilovaním TIA Portal odhalí nenastavené potrebné údaje a chyby, ktoré sa môžu vyskytnúť. Pri výskyte problému s kompiláciou je potrebné buď dané údaje doplniť, alebo zmeniť. Ak kompilovanie prebehne bez problémov je možné dané nastavenia nahrať do PLC, ako z LAN, tak aj z verejnej siete. Nahrávanie prebieha podobne ako pripojenie na PLC, kedy je potrebné zadať IP adresu kam sa majú údaje odoslať.

Po overení konfigurácie a prístupu k PLC z verejnej siete ostal radič zapojený, aby ho mohli vyhľadávače vyhľadať.

6.3 Zobrazenie informácii o PLC vo vyhľadávačoch

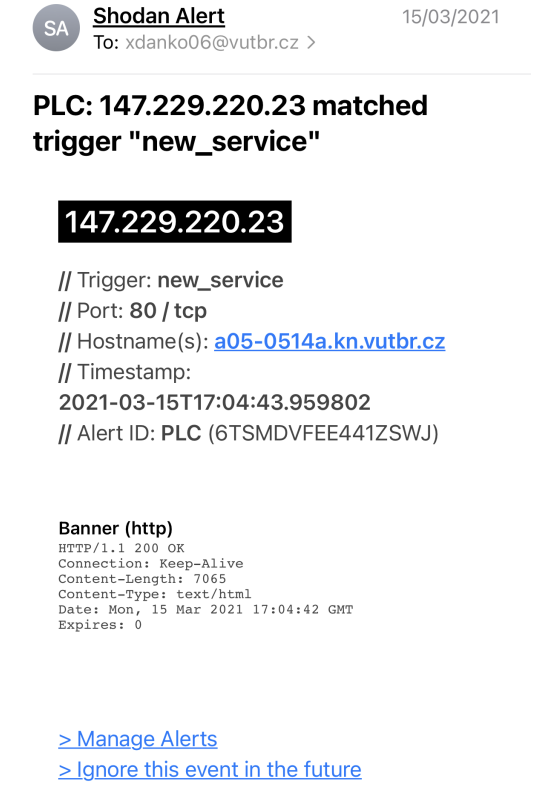
Zariadenie PLC bolo pripojené 03.03.2021 o 17:00. Vo vyhľadávači Shodan s akademickým účtom bol nadstavený Shodan monitor, ktorý umožňuje sledovať IP adresu. Pri každej zmene, ktorá nastane na sledovanej IP adrese Shodan odošle informácie o týchto zmenách na zvolený e-mail. Vďaka Shodan Monitoru nebolo potrebné každý deň sledovať vyhľadávač. Censys, BinaryEdge a ZommEye nemajú žiadnu takúto možnosť, preto bolo potrebné tieto vyhľadávače sledovať.

Prvý vyhľadávač, ktorý zaznamenal zapojené PLC bol Censys. Informácie o zapojenom PLC zariadení sa v tomto vyhľadávači objavili 20.03.2021, čo je 17 dní od jeho zapojenia. V informáciach sa nachádzali všetky dôležité informácie od IP adresy po verziu softvéru.

Ako druhý vyhľadávač, ktorý našiel zapojené PLC bol BinaryEdge. Informácie o PLC sa objavili v tomto vyhľadávači 26.03.2021, 23 dní po jeho zapojení. BinaryEdge dokázal taktiež vyhľadať všetky dôležité informácie ako Censys.

Zo Shodan vyhľadávača prišiel prvý e-mail 15.03.2021, 12 dní po jeho zapojení; konkrétne išlo o informáciu, že na danej IP adrese beží služba na porte 80. V e-maily sa nachádzajú rovnaké informácie ako pri samostatných výsledkoch v internetovom prehliadači od IP adresy po samostatný zachytený baner. Na obrázku 6.4 je možné vidieť ako e-mail s týmito informáciami vyzerá. Informácia `Alert ID` je označenie daného upozornenia pre sledovanú IP adresu, názov PLC bol zvolený pri nastavovaní

Shodan Monitoru. Údaj v zátvorke bol automaticky vygenerovaný a je ho potrebné používať v prípade, že chceme zmeny prijímať pomocou API alebo CLI.



Obr. 6.4: E-mail Shodan upozornenia.

Keď sa PLC vo výsledkoch vyhľadávača neobjavilo ani po dvoch mesiacoch, bola využitá možnosť skenovania IP adresy. Skenovaním požadovanej IP adresy sa skenujú na danej IP adrese všetky porty, ktoré Shodan prehľadáva okamžite po poslaní požiadavku o skenovanie. Nakoľko práca pomocou internetového rozhrania a API bola vyskúšaná so Shodan vyhľadávačom, skenovanie IP adresy bolo vykonané pomocou CLI. Aby bolo možné pristupovať k Shodan vyhľadávaču pomocou CLI je potrebné mať nainštalovaný Python a balíček Shodan. Shodan balíček je možné nainštalovať pomocou príkazu, ktorý je vo výpise 6.1.

Výpis 6.1: Inštalácia Shodan balíčka.

```
pip3 install -U --user shodan
```

Po úspešnej inštalácii je potrebné vykonať inicializáciu pomocou API kľúča a následne je možné zadať príkaz pre skenovanie IP adresy. Inicializácia a príkaz na skenovanie IP adresy spolu s odpoveďami sa nachádzajú vo výpise 6.2. Nakoľko je API kľúč súkromným údajom, vo výpise bol nahradený za `API_KEY`.

Výpis 6.2: Shodan inicializácia a skenovanie IP adresy.

```
PS D:\> shodan init API_KEY
Successfully initialized
PS D:\> shodan scan submit 147.229.220.23
Starting Shodan scan at 2021-05-06 14:24 - 99 scan credits
left
No open ports found or the host has been recently crawled
and cant get scanned again so soon.
```

Celkový sken IP adresy trval približne po dobu jednej hodiny, po ktorom prišla odpoveď, že na zadanej IP adrese sa nenachádza žiadny otvorený port alebo cieľová adresa už bola oskenovaná (odpoveď v anglickom jazyku sa nachádza vo výpise 6.2). Pre overenie či sa na danej adrese nachádzajú otvorené porty bolo teda potrebné použiť ďalší príkaz. Príkaz pre zobrazenie otvorených portov spolu s odpoveďou zo Shodanu sa nachádza vo výpise 6.3.

Výpis 6.3: Zoznam otvorených portov

```
PS D:\> shodan search --fields port 'ip:"147.229.220.23"'
22
23
1723
8291
```

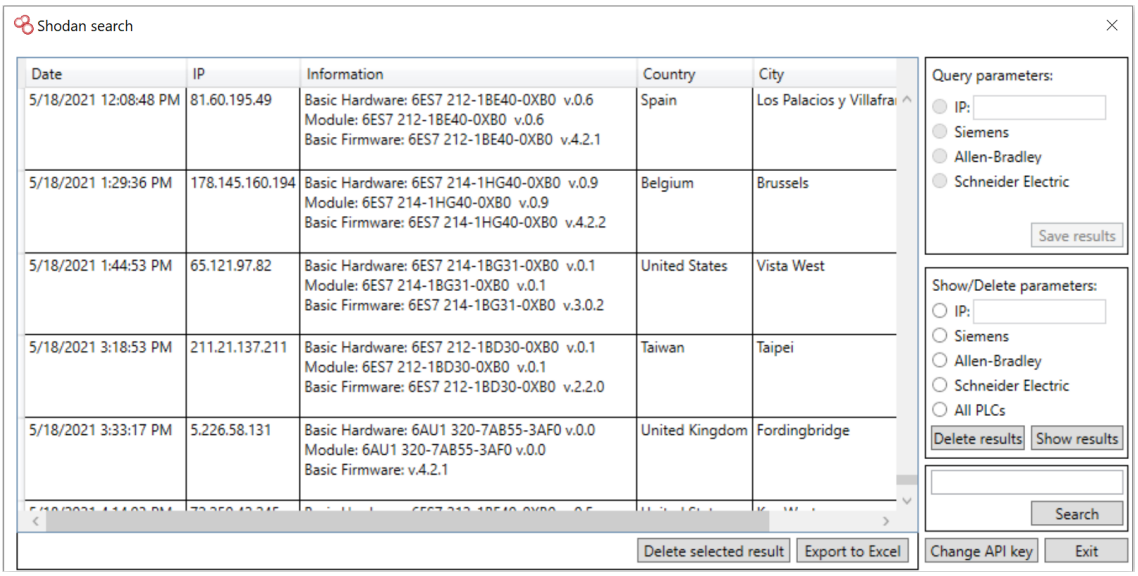
V zozname sa nenachádza port číslo 102, cez ktorý komunikujú Siemens PLC zariadenia, takže vyhľadávač nedokázal vyhľadať PLC zariadenie. Dôvody, pre ktoré Shodan nedokázal vyhľadať PLC sa nepodarilo nájsť a ani zistiť.

Vyhľadávač ZoomEye taktiež z neznámych dôvodov nedokázal vyhľadať PLC zariadenie a skenovať IP adresu v požadovanom momente tiež nebolo možné, pretože ZoomEye nedisponuje touto funkciou.

Posledný pokus vyhľadania PLC zariadenia na Shodan a ZoomEye vyhľadávači prebehol 26.05.2021, no ani v tomto prípade sa nepodarilo nájsť vo výsledkoch informácie o PLC zariadení.

6.4 Stiahnutie informácii o PLC pomocou aplikácie

Nakoľko Shodan nedokázal z neznámych dôvodov vyhľadať vlastné zapojené PLC, nebolo ani možné stiahnuť informácie pomocou vytvorenej aplikácie. Na obrázku 6.5 sa nachádza aspoň ukážka, ako a aké dáta zobrazuje aplikácia, ktorá je popísaná v kapitole 5.



Obr. 6.5: Aplikácia s výsledkami vyhľadávania.

V stĺpci `Information` sú informácie o PLC zariadení a je možné vidieť, že sa tam nachádza aj označenie firmvéru spolu s verziou. Ak sa objaví zraniteľnosť na danú verziu firmvéru, je možné pomocou aplikácie danú verziu vyhľadať a zistiť, ktoré PLC zariadenia sú zraniteľné.

6.5 Možné využitie informácií z pohľadu kybernetických zraniteľnosti

Vďaka informáciám z sa môže skúšať o útok pokúsiť aj osoba, ktorá nemá žiadne skúsenosti v oblasti OT. Nakoľko sa dá zistiť, na akej IP adrese sa nachádza PLC zariadenie je možné použiť voľno dostupné skripty. Tieto skripty nemusia výlučne zabezpečovať prístup do PLC zariadenia alebo meniť logiku vykonávaného procesu, môžu aj zbytočne zaťažovať PLC zariadenie, čo môže spôsobiť zvýšenie času odozvy.

Skúsenejší útočníci, ako napríklad operátory botnetov, by si pomocou aplikácie vedeli vyexportovať výsledky, a následne by mohli skúšať DDoS útok postupne na všetky IP adresy.

Ďalšia možnosť využitia týchto údajov je snaha o naviazanie pripojenia do PLC zariadení pomocou softvéru pre konfiguráciu. V prípade, že heslá nie sú dostatočne silné, môže sa útočník pokúsiť o slovníkový útok alebo brute–force útok k prístupu do PLC.

Aplikácia ukladá aj označenia zraniteľností, na ktoré je PLC zraniteľné. Doposiaľ sa vo výsledkoch neobjavilo žiadne zariadenie, ktoré by malo nejakú zraniteľnosť.

V prípade, že by sa takéto zariadenie objavilo v databáze, zahraničné spravodajské služby, ktoré majú zdroje a podporu zo strany štátu alebo autori škodlivého softvéry by vedeli vytvoriť malware využívajúci túto zraniteľnosť a zacieliť ho na dané zariadenie. Ak sa objaví zraniteľnosť na určitú verziu firmvéru ale Shodan ju nestihne priradiť k zariadeniam, v aplikácií je možné vyhľadať aj zariadenia s danou verziou firmvéru.

6.6 Možné riešenia skrytia informácii o PLC

Pokiaľ nie je vyhľadávač zariadení používaný napríklad na monitorovanie sietí, v ktorých sa PLC zariadenie nachádza, je z bezpečnostného hľadiska lepšie informácie o PLC skryť. Skrytie informácii pred vyhľadávačmi je možné niekoľkými spôsobmi, ako sú napríklad:

- IP Blacklist – vytvorenie IP Blacklistu vo firewalle s IP adresami vyhľadávačov je najjednoduchšie a najlacnejšie riešenie blokovania vyhľadávania. IP adresy vyhľadávačov sa však môžu meniť, a preto je potrebné sledovať IP adresy vyhľadávačov.
- IP Whitelist – vytvorenie IP Whitelistu vo firewalle je možné riešenie v prípade, že sa k PLC budú pripájať iba určité zariadenia so statickou IP adresou.
- Komunikačné brány – pri použití komunikačnej brány je PLC schované a dáta sa prenášajú pomocou iného protokolu.
- VPN – použitie VPN je najbezpečnejšie riešenie pripojenia PLC do verejnej siete. Náklady zapojenia však pri tomto riešení výrazne narastajú.

Závěr

Témou práce bolo získavanie informácií o priemyselných zariadeniach, konkrétne o PLC pomocou vyhľadávacích nástrojov zariadení. V teoretickej časti práce boli popísané prevádzkové technológie, ktoré tvoria základ priemyselných sieti, v ktorých sa nachádzajú priemyselné zariadenia. Tiež bola popísaná konvergencia prevádzkových a informačných technológií, ktorá sa za posledné roky v priemysle nesmierne rozšírila. S rastúcou popularitou konvergencie nastávajú aj potreby riešenia bezpečnosti priemyselných sietí a ich komponentov. Bezpečnosť priemyselných sietí bola popísaná okrajovo, pričom bol popis skôr zameraný na bezpečnosť PLC zariadení. Taktiež boli popísané základné informácie o najpoužívanejších protokoloch prevádzkových technológii, ktoré sa používajú pri PLC zariadeniach. Následne boli popísané vyhľadávacie nástroje zariadení, konkrétne Shodan, Censys, BinaryEdge a ZoomEye, ktoré dokážu zisťovať informácie o priemyselných zariadeniach pripojených do verejnej siete. Praktická časť práce bola rozdelená do štyroch kapitol. Kapitola 3 a 4 sa venuje prvému cieľu, kapitola 5 je zameraná na druhý cieľ a posledná kapitola 6 sa venuje tretiemu cieľu bakalárskej práce.

Prvý cieľ bol stanovený na porovnanie vyhľadávacích zariadení. Tento cieľ bol rozdelený na dve časti. Prvá časť sa venuje porovnaniu na základe dostupnej dokumentácie, informácií dostupných na webových stránkach vyhľadávačov a výsledkom vyhľadávania. Na základe dostupnej dokumentácie a informácií na webových stránkach sa prišlo k záveru, že na vyhľadávanie priemyselných zariadení je najlepšie používať vyhľadávače Shodan a ZoomEye. Porovnanie na základe výsledkov vyhľadávania prebiehalo pomocou webového rozhrania, kedy boli manuálne hľadané optimálne filtre pre zobrazenie informácií o PLC zariadeniach. Na základe výsledkov vyhľadávania je na hľadanie PLC zariadení najvhodnejší vyhľadávač BinaryEdge. Druhá časť sa venuje porovnaniu vyhľadávačov na základe práce s API. V tejto časti sa porovnávali iba vyhľadávače Shodan a ZoomEye, pretože Censys a BinaryEdge nevyhovovali požiadavkám pre vytvorenie aplikácie. Po porovnaní bol vybratý vyhľadávač Shodan z dôvodu možnosti mať zvýhodnený akademický účet so školskou e-mailovou adresou.

Druhý cieľ bol stanovený na vytvorenie aplikácie, ktorá bude využívať Shodan vyhľadávač na ukladanie výsledkov do databázy pomocou REST API. Aplikácie bola vytvorená v jazyku C# vo vývojovom prostredí Visual Studio 2019. Finálna verzia aplikácie je vytvorená vo WPF a dokáže sťahovať výsledky pomocou REST API, ukladať ich do SQL databázy a následne ich zobraziť buď hromadne, alebo filtrovane. Aplikácia dokáže výsledky aj exportovať do súboru Excel.

Tretím cieľom bolo zapojenie vlastného PLC zariadenia, aby sa zistilo, za ako dlho a aké informácie dokážu vyhľadávače Shodan, Censys, BinaryEdge a ZoomEye vyhľadať. PLC bolo zapojené do verejnej siete a bolo zistené, že vyhľadávače Censys a BinaryEdge, ktoré boli nevhodné pre tvorbu aplikácie boli jediné, ktoré dokázali vyhľadať zapojené PLC zariadenie. Následne boli navrhnuté spôsoby ako schovať zariadenie pred vyhľadávačmi.

Do budúcnosti by bolo vhodné zistiť dôvody, kvôli ktorým vyhľadávače Shodan a ZoomEye nedokázali vyhľadať PLC zariadenie zapojené do routeru, ktorý komunikoval s verejnou sieťou. Následne by sa dalo aplikáciu rozšíriť o ďalšie vyhľadávače, prípadne ju prerobiť do webovej aplikácie, ktoré sú v súčasnej dobe omnoho populárnejšie. Potenciálne rozšírenejšie v súčasnej dobe. Možné riešenia skrytia informácií by bolo možné rozšíriť o to, ako zmeniť informácie v prípade, že chceme, aby vyhľadávač dokázal vyhľadať PLC.

Literatúra

[1] 5 Industrial connectivity trends driving the IT-OT convergence. [online], ©2020, [cit. 2020-11-20].
URL https://iot-analytics.com/5-industrial-connectivity-trends-driving-the-it-ot-convergence/

[2] Ghaleb, A.; Zhioua, S.; Almulhem, A.: On PLC network security. *International Journal of Critical Infrastructure Protection*, ročník 22, 2018: s. 62–69, ISSN 1874-5482, doi:https://doi.org/10.1016/j.ijcip.2018.05.004, [cit. 2021-04-23].
URL https://www.sciencedirect.com/science/article/pii/S1874548215300421

[3] IT OT Convergence – Benefits and Challenges in Manufacturing. [online], ©2021, [cit. 2021-05-25].
URL https://www.tiempodev.com/blog/it-ot-convergence-benefits-and-challenges-in-manufacturing/

[4] Williamson, G.: OT, ICS, SCADA – What's the difference? [online], ©2004-2020, [cit. 2020-11-20].
URL https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

[5] What's the Difference Between OT, ICS, SCADA and DCS? - Insight from Securicon. [online], ©2018, [cit. 2020-11-20].
URL https://www.securicon.com/whats-the-difference-between-ot-ics-scada-and-dcs/

[6] International Conference on Computing, C. a. S.; Sudarsan, S. D.; Kumar, V.; aj.: *Proceedings on 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS): October 25th - 27th, 2018, Kathmandu, Nepal*. 2018, [cit. 2020-11-20].
URL https://ieeexplore.ieee.org/servlet/opac?punumber=8557205

[7] Bhamare, D.; Zolanvari, M.; Erbad, A.; aj.: Cybersecurity for industrial control systems. *Computers & Security*, ročník 89, 2020, ISSN 01674048, doi:10.1016/j.cose.2019.101677, [cit. 2020-11-20].
URL https://linkinghub.elsevier.com/retrieve/pii/S0167404819302172

[8] Mader, A.: A Classification of PLC Models and Applications. In *Discrete Event Systems*, Boston, MA: Springer US, 2000, ISBN 978-1-4613-7025-3, s. 239–246, doi:10.1007/978-1-4615-4493-7_24, [cit. 2021-04-22].
URL http://link.springer.com/10.1007/978-1-4615-4493-7_24

[9] Programmable Logic Controllers (PLCs): Basics, Types & Applications. [online], ©2020, [cit. 2020-11-21].
URL https://www.electrical4u.com/programmable-logic-controllers/

[10] Anderson, M.: What is RTU? ©2021, [cit. 2021-05-25].
URL https://realpars.com/rtu/

[11] Stouffer, K.; Pillitteri, V.; Lightman, S.; aj.: Guide to Industrial Control Systems (ICS) Security. Technická Zpráva NIST SP 800-82r2, National Institute of Standards and Technology, Červen 2015, doi:10.6028/NIST.SP.800-82r2, [cit. 2020-11-21].
URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[12] Colbert, E. J. M.; Kott, A. (editoři): *Cyber-security of SCADA and Other Industrial Control Systems*. číslo 66 in Advances in Information Security, Cham: Springer International Publishing : Imprint: Springer, první vydání, 2016, ISBN 9783319321257.

[13] Kant, D.; Creutzburg, R.; Johannsen, A.: Investigation of risks for Critical Infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan. *Electronic Imaging*, ročník 2020, č. 3, 2020-01-26: s. 253–1–253–16, ISSN 2470-1173, doi:10.2352/ISSN.2470-1173.2020.3.MOBMU-253, [cit. 2020-11-21].
URL https://www.ingentaconnect.com/content/10.2352/ISSN.2470-1173.2020.3.MOBMU-253

[14] Wiesel, C.: Design advice for connecting IT and OT. [online], ©2021, [cit. 2021-04-22].
URL https://www.controleng.com/articles/design-advice-for-connecting-it-and-ot/

[15] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Září 2016, [cit. 2021-04-23].
URL https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[16] Internationale Elektrotechnische Kommission (editor): *Industrial communication networks: network and system security. Pt. 1,1: Terminology, concepts and models*. číslo 62443-1-1 in International standard / IEC, Geneva: IEC Central Office, ed. 1.0, 2009-07 vydání, 2009, ISBN 9782889107100, oCLC: 931789715.

[17] Internationale Elektrotechnische Kommission (editor): *Industrial communication networks: network and system security. Pt. 3,3: System security requirements and security levels*. číslo 62443-3-3 in International standard / IEC, Geneva: IEC Central Office, ed. 1.0, 2013-08 vydání, 2013, ISBN 9782832210369.

[18] Joint Task Force Interagency Working Group: Security and Privacy Controls for Information Systems and Organizations. Technická zpráva, National Institute of Standards and Technology, Září 2020, doi:10.6028/NIST.SP.800-53r5, [cit. 2021-04-09].
URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[19] Stouffer, K. A.: *System protection profile - industrial control systems version 1.0*. NIST, version 1.0 vydání, 2004, doi:10.6028/nist.ir.7176, [cit. 2021-04-09].
URL http://dx.doi.org/10.6028/NIST.IR.7176

[20] *Pipeline SCADA Security*. Second ed. vydání, 2009.

[21] *Regulatory Guide 5.71*. First ed. vydání, 2010.

[22] *Risk-Based Performance Standards Guidance*. Washington, first ed. vydání, 2009.

[23] The top most used PLC Systems around the world. [online], ©2021, [cit. 2021-04-09].
URL https://engineering.electrical-equipment.org/electrical-distribution/the-top-most-used-plc-systems-around-the-world.html

[24] SCADA+ Pack. [online], ©2004-2019, [cit. 2021-04-22].
URL http://gleg.net/agora_scada.shtml

[25] YEW, W. C.: PLC Device Security – Tailoring need. 2014, [cit. 2021-04-22].
URL https://www.sans.org/reading-room/whitepapers/threats/plc-device-security-tailoring-37612

[26] Abbasi, A.; Hashemi, M.: Ghost in the PLC. [online], ©2021, [cit. 2021-04-23].
URL https://www.blackhat.com/docs/eu-16/materials/eu-16-Abbasi-Ghost-In-The-PLC-Designing-An-Undetectable-Programmable-Logic-Controller-Rootkit.pdf

[27] Houmb, S. H.: How to hack programmable logic controllers. [online], ©2004-2021, [cit. 2021-04-22].
URL https://www.controldesign.com/articles/2018/how-to-hack-programmable-logic-controllers

[28] Ginter, A.: The Top 20 CyberAttacks On Industrial Control Systems. ©2020, [cit. 2021-04-22].
URL https://waterfall-security.com/static/Top-20-ICS-Attacks.pdf

[29] Abbasi, A.; Hashemi, M.: Ghost in the plc designing an undetectable programmable logic controller rootkit via pin control attack. *Black Hat Europe*, ročník 2016, 2016: s. 1–35.

[30] Spenneberg, R.; Brüggemann, M.; Schwartke, H.: Plc-blaster: A worm living solely in the plc. *Black Hat Asia*, ročník 16, 2016: s. 1–16.

[31] Jeffries, B. M.: Securing Critical Infrastructure: A Ransomware Study. 2018.

[32] Mueller, P.; Yadegari, B.: The Stuxnet Worm. 2012, [cit. 2021-04-22].
URL `https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic9-final/report.pdf`

[33] Bencsáth, B.; Pék, G.; Buttyán, L.; aj.: Duqu: Analysis, detection, and lessons learned. In *ACM European Workshop on System Security (EuroSec)*, ročník 2012, Citeseer, 2012.

[34] Hemsley, K. E.; E. Fisher, D. R.: History of Industrial Control System Cyber Incidents. 12 2018, doi:10.2172/1505628, [cit. 2021-04-23].
URL `https://www.osti.gov/biblio/1505628`

[35] McMinn, L.; Butts, J.: A Firmware Verification Tool for Programmable Logic Controllers. In *Critical Infrastructure Protection VI*, editace J. Butts; S. Shenoi, Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, ISBN 978-3-642-35764-0, s. 59–69.

[36] Jr., A. M. G.: Firmware Modification Analysis in Programmable Logic Controllers. [online], March 2014, [cit. 2021-04-23].
URL `https://apps.dtic.mil/sti/pdfs/ADA599675.pdf`

[37] Carlsson, T.: Continued growth for industrial networks despite pandemic. ©2020, [cit. 2021-05-25].
URL `https://www.hms-networks.com/news-and-insights/news-from-hms/2021/03/31/continued-growth-for-industrial-networks-despite-pandemic`

[38] About Modbus Organization. [online], ©2002-2021, [cit. 2021-04-23].
URL `https://modbus.org/about_us.php`

[39] Clarke, G.; Reynders, D.; Wright, E.: *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*. Newnes, 2004.

[40] Communication by the Modbus protocol. [online], [cit. 2021-04-23].
URL `https://www.promotic.eu/en/pmdoc/Subsystems/Comm/Protocol/Modbus.htm`

[41] Difference between Modbus and Modbus Plus. [online], Leden 2012, [cit. 2021-04-23].
URL `https://program-plc.blogspot.com/2012/01/difference-between-modbus-and-modbus.html`

[42] S7comm. [online], 2016-05-13, [cit. 2021-04-09].
URL https://wiki.wireshark.org/S7comm

[43] Biham, E.; Bitan, S.; Carmel, A.; aj.: Rogue7: Rogue engineering-station attacks on S7 Simatic PLCs. *Black Hat USA*, 2019.

[44] PI North America. [online], ©2006-2021, [cit. 2021-04-23].
URL https://us.profinet.com/

[45] ODVA. [online], ©2021, [cit. 2021-04-23].
URL https://www.odva.org/

[46] EtherCAT - the Ethernet Fieldbus. [online], [cit. 2021-04-23].
URL https://www.ethercat.org/en/technology.html

[47] What is OPC UA? A practical introduction. [online], ©2021, [cit. 2021-04-09].
URL https://www.opc-router.com/what-is-opc-ua/#OPC-Specifications

[48] Overview of DNP3 Protocol. [online], ©2021, [cit. 2021-04-09].
URL https://www.dnp.org/About/Overview-of-DNP3-Protocol

[49] Jr., R. O.: Search engine exposes industrial-sized dangers. [online], ©2020, [cit. 2020-10-24].
URL https://www.smh.com.au/technology/search-engine-exposes-industrialsized-dangers-20120604-1zrnw.html

[50] Matherly, J.: *Complete Guide to Shodan*. Austin (Texas): Leanpub, 2016, [cit. 2020-10-03].
URL https://leanpub.com/shodan

[51] Bodenheim, R.; Butts, J.; Dunlap, S.; aj.: Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection*, ročník 7, č. 2, 2014: s. 114–123, ISSN 18745482, doi:10.1016/j.ijcip.2014.03.001, [cit. 2020-10-24].
URL https://linkinghub.elsevier.com/retrieve/pii/S1874548214000213

[52] Im, S.; Shin, S.; Roh, B.; aj.: Scan Modeling and Performance Analysis for Extensive Terminal Information Identification. *The Journal of Korean Institute of Communications and Information Sciences*, ročník 42, č. 4, 2017-04-30: s. 785–790, ISSN 1226-4717, doi:10.7840/kics.2017.42.4.785, [cit. 2020-10-24].
URL http://koreascience.or.kr/journal/view.jsp?kj=GCSHCI&py=2017&vnc=v42n4&sp=785

[53] Lee, S.; Shin, S.-H.; hee Roh, B.: Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning. In *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, IEEE, 2017, ISBN 978-1-5090-4749-9, s. 1048–1052, doi:10.1109/ICUFN.2017.7993960, [cit. 2020-10-24].
URL `http://ieeexplore.ieee.org/document/7993960/`

[54] Paganini, P.: Censys, the new search engine for the Internet's secrets. *Security Affairs - Read, think, share ... Security is everyone's responsibilitySecurity Affairs*, ročník 2015, 2015, [cit. 2020-10-25].
URL `https://securityaffairs.co/wordpress/42725/hacking/censys-search-engine.html`

[55] Durumeric, Z.; Adrian, D.; Mirian, A.; aj.: A Search Engine Backed by Internet-Wide Scanning. [online], Říjen 2015, [cit. 2020-10-10].
URL `https://censys.io/`

[56] Durumeric, Z.; Wustrow, E.; Halderman, J. A.: ZMap: Fast Internet-wide Scanning and Its Security Applications. In *22nd USENIX Security Symposium (USENIX Security 13)*, Washington, D.C.: USENIX Association, Srpen 2013, ISBN 978-1-931971-03-4, s. 605–620, [cit. 2021-04-09].
URL `https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/durumeric`

[57] Durumeric, Z.; Adrian, D.; Mirian, A.; aj.: A Search Engine Backed by Internet-Wide Scanning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*, New York, New York, USA: ACM Press, 2015, ISBN 9781450338325, s. 542–553, doi:10.1145/2810103.2813703, [cit. 2020-10-25].
URL `http://dl.acm.org/citation.cfm?doid=2810103.2813703`

[58] Internet Security Exposure 2016. [online], [cit. 2020-11-02].
URL `https://d1ehrggk1349y0.cloudfront.net/BinaryEdge-WorldReport.pdf`

[59] BinaryEdge. [online], [cit. 2020-11-02].
URL `https://www.binaryedge.io/`

[60] ZoomEye. [online], [cit. 2020-10-28].
URL `https://www.zoomeye.org/`

[61] Gill, J.: Zoomeye – Find open servers, Webcams, Porn sites vulnerabilities. [online], [cit. 2020-10-28].
URL `https://www.securitynewspaper.com/2018/12/25/zoomeye-find-open-servers-webcams-porn-sites-vulnerabilities/`

[62] Information Collection-Use of Zhong Kui's Eye. [online], © 2018-2020, [cit. 2020-10-28].
URL https://www.programmersought.com/article/93564990286/

[63] Postman. [online], ©2021, [cit. 2021-04-09].
URL https://www.postman.com/

[64] Lane, K.: Intro to APIs: What Is an API? [online], ©2021, [cit. 2021-04-09].
URL https://blog.postman.com/intro-to-apis-what-is-an-api/

Zoznam symbolov, veličín a skratiek

API	Application programming interface
BAS	Building automation system
CLI	Command Line Interface
CPU	Central processing unit
CVE	Common Vulnerabilities and Exposures
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service
DHT	Distributed hash table
DoS	Denial of Service
EMS	Energy management system
FEP	Front-end processor
HMI	Human Machine Interface
ICS	Industrial control systems
IDS	Intrusion Detection Systems
IED	Intelligent Electronic Device
IPS	Intrusion Prevention Systems
ISP	Internet service provider
IT	Information technology
NVD	National Vulnerability Database
OT	Operational technology
PCS	Process Control System
PLC	Programmable logic controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition

SCAP	Security Content Automation Protocol
SIS	Safety instrumented system
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual private network

A Tabuľka porovnania vyhľadávačov

Tabuľka obsahuje údaje porovnania vyhľadávačov na základe dokumentácie a informácii dostupných na webových stránkach jednotlivých vyhľadávačov.

	Shodan	**Censys**	**BinaryEdge**	**ZoomEye**
Rok založenia	2009	2015	2015	2013
Webová stránka	https://www.shodan.io/	https://censys.io/	https://www.binaryedge.io/	https://www.zoomeye.org/
IP adresy	IPv4, IPv6	IPv4	IPv4, IPv6	IPv4, IPv6
Nástroje vyhľadávania	Vlastný	ZMap, ZGrab a NMap	Neuvedené	XMap, WMap a NMap
Prístup k dátam	Webové rozhranie, CLI a API	Webové rozhranie a API	Webové rozhranie a API	Webové rozhranie a API
Protokoly a porty OT	Modbus: 502 Siemens S7: 102 DNP3: 20000 Niagara Fox: 1911, 4911 BACnet: 47808 EtherNet/IP: 44818 GE-SRTP: 18245, 18246 HART-IP: 5094 PCWorx: 1962 MELSEC-Q: 5006, 5007 OMRON FINS: 9600 Red lion: 789 CoDeSys: 2455 IEC 60870-5-104: 2404 ProConOs: 20547 MQTT: 1883	Modbus: 502 Siemens S7: 102 DNP3: 20000 Niagara Fox: 1911 BACnet/IP: 47808 MQTT: 1883	Neuvedené	Modbus: 502 Siemens S7: 102 DNP3: 20000 Niagara Fox: 1911 BACnet: 47808 Ethernet/IP: 44818 PCWorx: 1962 MELSEC-Q: 5006 OMRON FINS: 9600 Red lion: 789 IEC 60870-5-104: 2404 ProConOs: 20547 MQTT: 1883
HoneyPoty	Len honeyscore	Nie	Áno	Nie

Tab. A.1: Porovnanie vyhľadávačov na základe dokumentácie.

B Obsah priloženého média

Priložené médium obsahuje zložku `Aplikácia`, v ktorej sa nachádza zložka so zdrojovými kódmi `BakalarskaPracaXdanko06` a súbor pre otvorenie projektu vo Visual Studiu `BakalarskaPracaXdanko06.sln`. V priloženom médiu sa tiež nachádza elektronická verzia tejto práce a manuál k vytvorenej aplikácii.

- `/` ..... Koreňový adresár priloženého média
  - `Aplikácia` ..... Vytvorená aplikácia
    - `BakalarskaPracaXdanko06` ..... Zdrojové kódy aplikácie
      - `Properties`
        - `AssemblyInfo.cs`
        - `Resources.Designer.cs`
        - `Resources.resx`
        - `Settings.Designer.cs`
        - `Settings.settings`
      - `App.config`
      - `App.xaml`
      - `App.xaml.cs`
      - `BakalarskaPracaXdanko06.csproj`
      - `DataAccessLayer.cs`
      - `DataParser.cs`
      - `DbRepo.dbml`
      - `DBRepo.dbml.layout`
      - `DbRepo.designer.cs`
      - `ExportData.cs`
      - `MainWindow.xaml .4 MainWindow.xaml.cs`
      - `packages.config`
      - `shodan.ico`
      - `ShodanAPI.cs`
      - `ShodanSearch.xaml`
      - `ShodanSearch.xaml.cs`
    - `BakalarskaPracaXdanko06.sln` ..... Súbor pre otvorenie projektu
  - `BakalarskaPraca.pdf` ..... Elektronická kópia tejto práce
  - `Manual.pdf` ..... Manuál k vytvorenej aplikácii